



THIRD EDITION

Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising and Marketing





Privacy Law: A Global Legal Perspective
on Data Protection Relating to Advertising and Marketing

THIRD EDITION

This publication provides general guidance only. It does not provide legal advice.
Please consult your attorney for legal advice.

©2025 Global Advertising Lawyers Alliance

FOREWORD

Since the last edition of this book in 2022, the legal and technological landscape for advertising and marketing has shifted dramatically. The rapid adoption of artificial intelligence, the tightening control of platforms and browsers on data flows, and a surge of new and strengthened privacy laws around the world have reshaped how brands, agencies, publishers, and platforms understand and connect with consumers. Data remains the lifeblood of the advertising ecosystem, powering research and analytics, attribution and measurement, personalized marketing, and entirely new ways to reach audiences, but the rules governing that data are evolving at unprecedented speed.

The past three years have seen privacy and data protection move even further from a compliance obligation to a strategic business priority. Dozens of jurisdictions have enacted or strengthened comprehensive privacy frameworks, many modeled on the GDPR but increasingly going beyond it with stricter consent standards for targeted advertising, broader definitions of personal data, and AI-specific obligations. In the United States alone, the number of state privacy laws has more than doubled, adding expanded rights for sensitive data, enhanced opt-out mechanisms for targeted advertising, and heightened enforcement. Countries across Asia, Africa, and Latin America have followed suit, many introducing stringent cross-border transfer restrictions and data localization mandates that complicate global campaigns.

At the same time, enforcement activity has accelerated. Regulators are issuing record fines for unlawful profiling, noncompliance with transparency and consent obligations, and violations of children's privacy. Privacy enforcement is also converging with competition and consumer protection law, changing how authorities assess the fairness of data-driven advertising practices. For advertisers, this means compliance now requires a more holistic view of legal risk, spanning privacy, market competition, and consumer trust.

And then there's AI. Generative AI and predictive analytics tools are now embedded in advertising workflows, from creative generation to media buying, raising fresh questions about lawful data sourcing, fairness, bias mitigation, and accountability. Regulators are

signaling that existing privacy and marketing rules apply with full force to these tools, and in some jurisdictions, AI-specific obligations aimed at ensuring transparency, human oversight, and ethical use have been layered on top.

This third edition of *Privacy Law and Data Protection: A Global Legal Perspective on Advertising and Marketing*, produced by the Global Advertising Lawyers Alliance (GALA), remains unmatched in scope and focus: a comprehensive, jurisdiction-by-jurisdiction guide to privacy and data protection laws in the advertising and marketing sector, written by leading local experts in 78 countries. Each chapter provides the legal framework, practical implications for advertisers, and insights into where the law is heading.

On behalf of GALA, I am grateful to every contributor for the time, expertise, and clarity they brought to this work. In a world where laws, technology, and public expectations continue to evolve at a rapid pace, we hope this 2025 edition serves as an essential, authoritative resource for navigating the complex intersection of privacy, data protection, and advertising law.

Daniel Goldberg
Frankfurt Kurnit Klein & Selz, PC

September 2025

ABOUT GALA

The Global Advertising Lawyers Alliance (GALA) is the leading network of advertising lawyers in the world. With firms representing more than 90 countries, each member has the local expertise and experience in advertising, marketing and promotion law that will help your campaign achieve its objectives, and navigate the legal minefield successfully. GALA is a uniquely sensitive global resource whose members maintain frequent contact with each other to maximize the effectiveness of their collaborative efforts for their shared clients. GALA provides the premier worldwide resource to advertisers and agencies seeking solutions to problems involving the complex legal issues affecting today's marketplace.

For further information about GALA, please contact the relevant member directly or alternatively GALA's Executive Director, Stacy Bess at:

Global Advertising Lawyers Alliance

28 Liberty Street, 35th Floor, New York, NY 10005

Tel: 212.705.4895 | Fax: 347.438.2185

Email: sbess@galalaw.com

www.galalaw.com

TABLE OF CONTENTS

Algeria	11
Argentina	19
Australia	30
Belize	49
Bolivia	64
Bosnia and Herzegovina	74
Brazil	88
Canada	107
Chile	124
China	138
Colombia	154
Costa Rica	166
Curaçao	175
Dominican Republic	186
Ecuador	203
Egypt	221
El Salvador	228
European Union	238
Austria	257
Belgium	267
Bulgaria	278
Croatia	291
Cyprus	303
Czech Republic	311

Denmark	327
Finland	337
France	346
Germany	358
Greece	374
Hungary	384
Ireland	394
Italy	403
Latvia	418
Lithuania	427
Luxembourg	437
Malta	449
Netherlands	456
Poland	470
Portugal	484
Romania	494
Slovakia	506
Spain	515
Sweden	528
Ghana	544
Guatemala	557
Honduras	572
Hong Kong	579
India	596
Israel	608

Jamaica	618
Japan	632
Kenya	650
Malaysia	669
Mexico	681
Morocco	695
New Zealand	703
Nicaragua	718
Nigeria	732
North Macedonia	743
Norway	759
Paraguay	768
Peru	777
Puerto Rico	788
Rwanda	798
Serbia	817
Singapore	834
South Africa	851
South Korea	867
Switzerland	885
Trinidad and Tobago	903
Tunisia	916
Turkey	924
Uganda	942
Ukraine	957



United Kingdom	976
United States of America	992
Uruguay	1014
Venezuela	1030
Zimbabwe	1038
List of GALA Members	1049

ALGERIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Algeria.

Privacy in Algeria is regulated under Law No 18-07 which establishes the legal framework for the protection of personal data ('Personal Data Protection Law'). This law provides principles governing data processing activities, ensuring that personal data is handled in a manner that respects individual rights and privacy. The law applies to public and private entities processing personal data within Algeria, and mandates compliance with data security and consent requirements. The National Authority for the Protection of Personal Data is the primary regulatory body overseeing enforcement and compliance.

1.2 What are the primary laws regulating privacy in Algeria? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

In addition to the Personal Data Protection Law, other relevant laws include:

- Law No 09-04 on Cybercrime, which includes provisions related to unauthorized data access;
- the Criminal Code, which penalizes unauthorized data processing; and
- Law No 15-04 on Electronic Signature and Certification, which governs digital transactions.

Sector-specific regulations may apply to financial services, healthcare, and telecommunications, particularly regarding data processing and retention.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation is not explicitly mandated under Algerian privacy law. However, businesses engaged in advertising, particularly digital marketing, are expected to adopt internal compliance measures to align with legal requirements. Industry associations and multinational corporations operating in Algeria often implement self-regulatory guidelines that complement national laws.

1.4 How is privacy law enforced in Algeria? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The National Authority for the Protection of Personal Data is responsible for enforcing privacy laws. It has the authority to investigate violations, impose administrative sanctions, and refer cases for prosecution when necessary. Privacy violations may also be pursued under Algeria's criminal law, with potential penalties including fines and imprisonment. There is no private right of action for individuals; enforcement is primarily handled by regulatory authorities.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Algeria?

A company is subject to Algerian privacy law if it processes personal data within Algeria, regardless of whether it is a local or foreign entity. The law applies to both private and public sector entities handling personal data, requiring them to comply with data protection principles, security measures, and

consent requirements.

2.2 Does privacy law in Algeria apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, Algerian privacy law applies to foreign companies that process the personal data of Algerian residents, particularly if they use infrastructure in Algeria or target Algerian consumers. Foreign companies may be required to appoint a local representative or obtain authorization from the National Authority for the Protection of Personal Data when engaging in data processing activities involving Algerian data subjects.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Algeria?

‘Personal data’ is defined as any information that directly or indirectly identifies a natural person. This includes names, identification numbers, biometric data, financial information, and digital identifiers.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive personal data’ includes racial or ethnic origin, religious beliefs, political opinions, health status, genetic data, biometric data, and criminal records. The processing of sensitive data requires explicit consent from the data subject or must be justified by a legal exemption.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized data that cannot be re-identified is not subject to privacy law. However, pseudonymized data that can be linked back to an individual is still considered personal data and remains subject to legal protection.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must obtain consent before processing personal data, limit data collection to necessary purposes, implement security measures, provide privacy notices to individuals, and maintain records of data processing activities. Organizations must also ensure proper training for employees handling personal data.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, companies are categorized as either data controllers or data processors. Data controllers determine the purposes and means of processing, while data processors handle data on behalf of controllers and must adhere to contractual security obligations.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, data processing must be based on consent, legal obligations, contractual necessity, or legitimate interest, provided that it does not infringe on individuals' privacy rights.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Privacy notices must specify the purpose of data collection, legal basis for processing, data retention period, individuals' rights, and contact details for inquiries.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the right to access, correct, and delete their data, withdraw consent, and object to the use of their data for marketing purposes.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies must obtain explicit opt-in consent for direct marketing via electronic communications and provide an easy opt-out mechanism for consumers.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Controllers must ensure that vendors implement security, confidentiality and lawful processing measures. Contracts are required to clarify roles and obligations in compliance with the Personal Data Protection Law.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Contracts must include clauses on data use limitation, confidentiality, technical safeguards, breach notification, and restrictions on international transfers.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Data protection impact assessments are required for high risk processing activities, especially in digital marketing involving profiling, tracking, or sensitive data use.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing activities require prior consent from individuals. Companies must provide clear opt-in mechanisms before sending marketing communications. Additionally, recipients must be offered a straightforward way to opt out of future communications at any time.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies requires user consent. Websites and mobile applications must disclose their use of cookies and provide users with options to accept, reject, or customize tracking settings. The National Authority for the Protection of Personal Data may issue further guidance on the matter.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs must adhere to data minimization and purpose limitation principles. Consumers must be informed about how their data will be processed, stored, and shared. Consent must be obtained before using personal data for marketing or profiling within loyalty programs.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing campaigns must comply with data protection regulations. Any collection or processing of user data for targeting purposes must be disclosed, and consent must be obtained. Transparency about sponsored content is also required.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising based on behavioral tracking requires explicit consent from users. Advertisers must allow individuals to opt out of tracking. Contextual advertising, which does not involve personal data, is generally subject to fewer legal restrictions.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no explicit laws governing digital identity resolution or clean room technologies in Algeria. However, general data protection principles apply, requiring organizations to ensure data security and transparency in processing personal data.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising requires user consent before collecting geolocation data. Companies must inform users about how their location data will be used and provide options to disable location tracking.

7.8 How are data brokers defined and regulated under privacy law?

Algerian privacy law does not provide a specific definition for data brokers. However, entities collecting and selling consumer data must obtain the appropriate regulatory approvals and comply with data processing regulations.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising targeting minors is subject to stricter regulations, including obtaining parental consent before collecting or processing data of children under a certain age. Behavioral tracking of minors is generally prohibited.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Profiling and AI-driven advertising must comply with transparency and fairness principles. Individuals must be informed when AI-based decision-making affects them and must have the option to challenge automated decisions.

7.11 Are there other specific advertising practices that you wish to discuss?

Businesses must remain compliant with any future amendments to Algerian privacy laws, especially in emerging areas such as biometric advertising and AI-based consumer engagement.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The transfer of personal data outside Algeria requires authorization from the National Authority for the Protection of Personal Data. Companies must demonstrate that the recipient country provides an adequate level of protection or implement contractual safeguards, such as standard contractual clauses.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Sensitive personal data transfers may require additional security measures, such as encryption. Legal and professional privilege considerations must be evaluated to ensure compliance with confidentiality obligations.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Algeria? Are there minimum standards? Does this differ by sector or size of the entity?

Organizations must implement technical and organizational security measures to protect personal data from unauthorized access and breaches. Certain sectors, such as finance and healthcare, may have stricter security standards.

9.2 How are personal data breaches regulated in Algeria? What are the requirements for notification and response?

There is no mandatory data breach notification requirement under Algerian law. However, companies are encouraged to report breaches affecting individuals' rights to the National Authority for the Protection of Personal Data.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Non-compliance with privacy laws can result in fines and, in severe cases, criminal penalties, including imprisonment for unauthorized data processing or transfers.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers do not have a direct private right of action but may file complaints with the regulatory authority, which can take enforcement actions.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement activity is increasing, with authorities focusing on unauthorized data processing and breaches of confidentiality in digital advertising and financial services.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Algeria?

Privacy laws in Algeria reflect strong national security interests, with government agencies maintaining broad access to personal data.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Companies should monitor potential amendments aligning Algeria's laws with international standards, particularly regarding cross-border data transfers and AI-based data processing.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Businesses should conduct periodic compliance assessments to ensure adherence to evolving privacy regulations.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There is an increasing focus on AI regulation and stronger enforcement measures by the National Authority for the Protection of Personal Data.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Challenges include navigating data transfer restrictions, obtaining regulatory approvals, and ensuring AI-driven processing complies with transparency requirements.

12.3 What do you envision the privacy landscape will look like in five years?

Privacy laws are expected to evolve toward stricter regulatory compliance, including mandatory breach notification and expanded consumer rights protections.

ARGENTINA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Argentina.

Privacy rights were incorporated into the Argentine legal system with the 1994 constitutional reform, as the result of the incorporation of the *habeas data* procedure. Since then, privacy rights have acquired constitutional protection, being considered as fundamental rights that cannot be suppressed or restricted without sufficient cause. In addition, the National Civil and Commercial Code and several international treaties executed by Argentina have recognized privacy rights as fundamental rights.

In general terms, the Argentine data protection system follows the European legal regime. On January 15, 2024, the European Commission ratified that Argentina grants an adequate level of protection for personal data transferred from the European Union.

1.2 What are the primary laws regulating privacy in Argentina? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The current legal framework regulating privacy is vast and complex; the main regulations—including those focusing on advertising aspects—are as follows:

- (a) Data Protection Law No 25,326 ('DPL');
- (b) DPL Regulatory Decree 1558/2001 ('Regulatory Decree');
- (c) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') and its additional protocol ('Convention 108+'). Convention 108+ will enter into force for those countries which have ratified it, provided that it has at least 38 parties;
- (e) Provisions issued by the Access to Public Information Agency ('APIA');
- (f) Law No 26,951 (the 'Do-Not-Call Law'), creating the 'Do-Not-Call Registry' and expanding the protection of data owners' rights (see question 5.2);

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation does not have a significant role in the privacy regulation.

1.4 How is privacy law enforced in Argentina? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The National Directorate for Personal Data Protection ('NDPDP'), part of the National Department of Justice and Human Rights, was formed in 2001 and was previously the data protection authority. However, Emergency Decree 746/2017 replaced it with the APIA.

Among other responsibilities, the APIA is responsible for:

- (a) operating a registry of databases (keeping records of the registration of databases);
- (b) enforcing the DPL and the Do-Not-Call Law, carrying out inspections and imposing sanctions; and
- (c) creating new dispositions and regulations related to data protection matters.

The APIA is also responsible for ensuring the effective exercise of the right of access to public information and the enforcement of transparency within the public sector.

The APIA's inspections/audit proceedings can be *ex officio* or initiated upon a complaint. The administrative process that the APIA must follow to investigate and impose penalties is set out in the DPL, the Regulatory Decree and in Decree 1160/2010. Administrative decisions can be appealed before the judicial courts.

In addition to the APIA, there are specific regulators for certain industry sectors, such as the Argentine Central Bank ('BCRA') which regulates data handled by financial institutions. There are also many non-governmental organizations ('NGO's) exclusively dedicated to data protection matters, but with no enforcement authority, such as: Argentina Cyber Secure (www.argentinacibersegura.org/); Association for the Civil Rights (adc.org.ar/) and Argentina Internet Chamber (www.cabase.org.ar/), among others.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Argentina?

The DPL applies to individuals or legal entities carrying out the processing of personal data of Argentinean residents or processing that produces effects in Argentina, regardless of where such processing is performed.

Pursuant to the DPL, the registration of databases is a legal requirement which is mandatory for all data controllers and processors under the scope of the DPL.

2.2 Does privacy law in Argentina apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, companies outside the country that process the data of Argentinean residents or carry out processing that produces effects in Argentina must comply with local law and regulations.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Argentina?

'Personal data' is defined by the DPL as any type of information that relates to identified or identifiable individuals or legal entities.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

'Sensitive data' is defined in the DPL as any personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to the health or sexual life of an individual. As a general principle, sensitive data collection, processing and/or treatment is forbidden unless expressly authorized by law.

Individuals cannot be compelled to provide sensitive data. Moreover, sensitive data can only be collected and/or treated in cases where there are circumstances of general interest authorized by law, or for statistical or scientific purposes, provided that data owners cannot be identified. Section 7 also provides that it is prohibited to create files, banks or registers storing information that directly or indirectly reveals sensitive data. Notwithstanding, the Catholic Church, religious associations, and political and labor organizations are entitled to keep a register of their members.

Public or private health institutions, as well as medical science professionals, are entitled to collect and treat such personal data as relate to the physical or mental condition of patients who make use of their services, or who are or have been in their care, in pursuance of the principles of professional confidentiality.

Furthermore, data referring to criminal records can be treated only by the competent public authorities, within the framework established by the corresponding laws and regulations.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The DPL defines ‘data dissociation’ as any processing of personal data in such a way that the information obtained cannot be associated with a specific or identifiable person. Moreover, Resolution 4/2019 of the APIA provides that a person shall not be considered as an identifiable person, under the terms of the DPL, when the procedure to achieve their identification requires the application of disproportionate or unfeasible measures or deadlines.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The following fundamental principles apply to data processing, namely:

- (a) personal data collected must be true, adequate, relevant, and not excessive in relation to the scope and purpose for which the data has been obtained;
- (b) the collection of personal data cannot be done by unfair or fraudulent means;
- (c) personal data subject to treatment cannot be used for purposes different from or incompatible with the purposes for which it was collected;
- (d) personal data must be stored in such a way as enables data owners to exercise their right of access;
- (e) the data must be destroyed once it has ceased to be necessary or relevant to the purposes for which it has been collected; and
- (f) those responsible or involved in any part of data processing are bound by the duty of confidentiality.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The DPL establishes that when personal data processing services are provided on behalf of third parties, such data may not be applied or used for a purpose other than that stated in the service contract; and, once the contractual provision has been fulfilled, the processed personal data must be destroyed, except with the express authorization of the party on whose behalf such services are provided when it is reasonably presumed that further orders may be made, in which case they may be stored under the appropriate security conditions for a period of up to two years. Furthermore, the Regulatory Decree establishes that the contract binding the processor to the controller must provide that:

- (a) the processor acts only on instructions from the controller; and
- (b) the security obligations of the DPL are also applicable to the processor.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The DPL states that a data subject must give express consent to the collection and processing of personal data. This consent must be:

- given freely;
- based on information provided to the data owner in advance; and
- expressed in writing or in an equivalent form.

The controller must inform the data subject of:

- (a) the purpose for which the data will be processed, and who their addressees or type of addressees may be;
- (b) the existence of the relevant database, and the identity and address of the person responsible for it;
- (c) whether the answers to the questionnaire submitted are mandatory or optional, in particular regarding sensitive data;
- (d) the consequences of:
 - (i) providing the data,
 - (ii) refusal to do so, or
 - (iii) inaccuracy of the data; and
- (e) the possibility for the data subject to exercise their right of data access, rectification and deletion.

Consent is not necessary in specific circumstances. Legitimate interest is not provided in the DPL as a lawful basis for processing.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

By Disposition 4/2009, all marketing communications in Argentina must include:

- (a) information to recipients on their right to request their exclusion from the relevant database;
- (b) an opt-out mechanism; and
- (c) two legal transcriptions (in Spanish).

Unsolicited communications, or those sent without consent, must evidence their marketing nature in a noticeable manner. For emails, their subject field must read 'Publicidad' ('Advertisement') and cannot include anything else.

Companies carrying out direct marketing campaigns must ensure that they implement effective mechanisms to fulfil all potential opt-out requests.

Disposition 18/2015, approving the 'Privacy Good Practice Guide for the Development of Apps and Software' which establishes that a privacy policy should be clear and easily accessible for users. In addition, the privacy policy for apps designed for use on phones or tablets must be shown in a useful way for users, bearing in mind the size restrictions that apply to these devices.

Resolution 14/2018 establishes that the owners and users of public and private databases must, prior to the collection of the data, clearly and expressly exhibit, in a visible place, the information described in question 4.3(a)–(e) above, making particular reference to the way in which data subjects may exercise their rights.

Likewise, the following wording must be included: ‘LA AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, en su carácter de Órgano de Control de la Ley No 25.326, tiene la atribución de atender las denuncias y reclamos que interpongan quienes resulten afectados en sus derechos por incumplimiento de las normas vigentes en materia de protección de datos personales’ (‘THE AGENCY OF ACCESS TO PUBLIC INFORMATION, as the Controlling Authority of Law No 25,326, has the attribution of attending to any claims and allegations filed by those affected in their rights for non-compliance with the current data protection regulation’).

These requirements apply to all marketing addressed to Argentine residents, irrespective of the country or jurisdiction from which the marketing communications are delivered.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

In addition to the rights of access, rectification and deletion, in 2014, the Do-Not-Call Law created the Do Not-Call Registry, expanding the protection of data owners’ rights. This regulation allows the data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephone must register with the Agency and check on a monthly basis the list of blocked numbers before engaging in marketing calls.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

All marketing communications in Argentina must include:

- (a) information to recipients on their right to request their exclusion from the relevant database;
- (b) an opt-out mechanism; and
- (c) two legal transcriptions (in Spanish).

Unsolicited communications, or those sent without consent, must evidence their marketing nature in a noticeable manner. For emails, their subject field must read ‘Advertisement’ and cannot include anything else.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The use of vendor and other third parties in advertising is not specifically regulated. However, general principles arising from the DPL and its regulations and dispositions apply also to such advertising.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Please refer to question 4.2.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must comply with the obligations arising from the Argentine legal data protection framework.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Please refer to answers in questions 5.1. and 5.2.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of cookies, pixels and other tracking technologies has not yet been regulated, nor particularly addressed in any APIA recommendation. However, applying the DPL's principles, companies trying to obtain information through tracking technologies must obtain the user's consent to collect information.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions are subject to the rights and obligations arising from the data protection legal framework.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media is not specifically regulated. However, general principles arising from the DPL and its regulations and dispositions apply also to social media.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising and behavioral advertising are not specifically regulated by local law. However, the regulations discussed in questions 5.1 and 5.2 also apply to these type of advertising activities.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room are not specifically regulated. However, general principles arising from the DPL and its regulations and dispositions apply also to them.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not specifically regulated. However, general principles arising from the DPL and its regulations and dispositions apply also to it.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are not specifically regulated by local privacy law.

7.9 How is advertising to children and minors regulated under privacy law?

The DPL does not include specific provision for children and minors. Resolution 4/2019 of the APIA states that, in the case of processing personal data of children and adolescents:

- (a) pursuant to the principle of progressive autonomy included in the National Civil and Commercial Code, a minor may provide informed consent in relation to the processing of their personal data, taking into consideration their psycho-physical characteristics, aptitudes and development; and
- (b) if the minor does not have sufficient capacity to provide informed consent, the holder of parental responsibility or guardianship over the child or adolescent must provide consent for the processing of their personal data. In such a case, the controller must make such efforts to verify that consent has indeed been given by the person holding parental responsibility or guardianship over the child or adolescent as are reasonable in the circumstances.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

In the framework of the APIA's National Program on Transparency and Protection of Personal Data in the use of Artificial Intelligence (Resolution 161/2023), a draft version of the Guide for Public and Private Entities on Transparency and Protection of Personal Data for responsible Artificial Intelligence was published. The APIA indicated that this tool was developed to address the full lifecycle of AI systems, their design, implementation and maintenance. It focuses on two main aspects: algorithmic transparency and personal data protection. A deadline for comments and recommendations was set for October 30, 2024. The final version of the report has not yet been published.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The DPL forbids any transfer of personal data of any kind to countries or international or 'supranational' organizations that do not grant an adequate level of protection pursuant to the APIA's standards. The list of countries considered as having 'adequate' level protection includes: the member states of the EU and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faroe Islands, Canada (only private sector), New Zealand, Andorra, Uruguay, Israel (automated data treatment only) and the UK.

Such prohibition does not apply where:

- (a) the data subject has given express consent, by authorizing the international transfer of their personal data (including to countries not granting 'adequate levels of protection'), or
- (b) an adequate level of protection arises from contractual clauses or self-regulation systems of the data assignor and data assignee (such as binding corporate rules, global policies or codes of conduct).

Disposition 60/2016 approved two sets of standard model clauses for data controller to data controller transfers as well as data controller to data processor transfers. These models are based on the EU Model Contracts for the transfer of personal data to third countries. Moreover, by Resolution 198/2023, the APIA incorporated into the applicable legal framework in Argentina the standard contractual clauses for international data transfers of the Ibero-American Data Protection Network. Any of these options are valid to comply with the requirements of the DPL.

Furthermore, Resolution 159/2018 issued by the APIA sets out 'Guidelines and Basic Contents of Binding Corporate Rules' for the international free flow of personal data among companies of the same economic group. The guidelines are aligned with Section 47 of the GDPR, addressing issues such as basic conditions for the legality of the transfer, procedures to ensure data subjects' rights, joint liability of parties, applicable jurisdiction in case of controversies and APIA auditing rights.

Argentine companies transferring personal data to affiliates in countries without 'adequate' personal data legislation, based on corporate rules other than those established by Resolution 159/2018, must submit them to the APIA for its approval.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Argentina? Are there minimum standards? Does this differ by sector or size of the entity?

The DPL states that companies must adopt the necessary technical measures to guarantee the protection and confidentiality of data, to prevent any adulteration, loss or unauthorized access or processing.

In 2018, the APIA issued Resolution 47/2018, which approved two sets of recommended security measures for the processing and conservation of personal data. It includes general recommendations in relation to personal data stored by electronic and non-electronic means, regardless of the sector or size of the company.

In principle, Resolution 47/2018 establishes a set of recommendations that can be adopted or replaced by other more effective measures based on the practices and circumstances of the processing of personal data. Thus, although the measures provided by Resolution 47/2018 are not strictly binding, the standards provided in the Resolution may be considered to be the minimum levels any controller or processor must meet to comply with the DPL.

9.2 How are personal data breaches regulated in Argentina? What are the requirements for notification and response?

The obligation to report data security incidents is not legally established. Under the DPL, there is no specific legal obligation to report data breaches to authorities. However, Resolution 47/2018 includes the practice of recording security breaches and communicating them to the APIA, with specific requirements, and, as stated in question 9.1 above, this may be considered to be a minimum level any controller or processor must meet to comply with the DPL.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties are established in Sections 31 and 32 of the DPL and in the Regulatory Decree. The APIA may apply sanctions for any violations of the Argentine data protection legal framework. The sanctions can include warnings, suspensions, fines and closure or erasure of the database, without prejudice to any applicable civil or criminal liabilities. There are also precedents for the authority fining companies which fail to comply with the data protection legislation, although such fines are usually low.

In addition, any person who:

- (a) has knowingly provided false information contained in a personal data file to a third party;
- (b) has knowingly and unlawfully, or by violating data confidentiality and security systems, accessed a personal database;
- (c) has unlawfully provided or disclosed to third parties information registered in a personal database that should be kept confidential by provision of law; or
- (d) has unlawfully inserted data in a database,

may be imprisoned for a term of between one month and two years.

Penalties imposed will be increased if the perpetrator is a public officer.

10.2 Do consumers have a private right of action? What remedies are available to them?

Anyone with a legitimate interest—whether an individual or a company—may file an administrative claim before the APIA. The APIA may also start a preliminary investigation *ex parte*. Pursuant to the regular process set out in the Administrative Proceedings Regulation, administrative decisions can be appealed before the judicial courts.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

As anticipated, the APIA has imposed a large number of sanctions for breaches of the Do-Not-Call Law. However, apart from this, the APIA has not imposed a large number of sanctions for breaches of the personal data regulation in recent years. The most significant cases were caused by security incidents that became public, and the APIA then set about investigating the facts. Sanctions have also been issued for non-compliance in the exercise of data subjects' rights.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Argentina?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

On June 30, 2023, during the previous presidency before Javier Milei's current administration, the final version of the Personal Data Protection Bill ('Bill'), to update the DPL (enacted in 2000), was sent to the National Chamber of Deputies.

The accompanying Message stated that ‘after more than 20 years, the National State requires its regulations to be updated in order to strengthen the State’s regulatory and public policy management capacities with the aim of responding to the new challenges imposed by technological innovations and the development of the digital economy and, at the same time, to be in line with regional and international standards...’.

The Bill was promoted by the APIA, and is the result of a public consultation process, under which the opinions, contributions and comments of both the private sector and the national and international public sector were received.

The Bill:

- (a) introduces new definitions, aligned with both the GDPR, and the Brazilian data protection regulation, such as database, personal data and sensitive data;
- (b) introduces new concepts regarding genetic data, biometric data, economic groups, security incidents and international transfer;
- (c) limits the scope of ‘data subjects’ to human persons;
- (d) provides new grounds for the collection and processing of personal data other than consent, such as legitimate interests;
- (e) introduces the obligation to report any security incident to the controlling authority and to data subjects; and
- (f) increases exponentially the penalties for infringements.

There are other drafts laws which have been presented in Congress by different political parties, all very similar to the Bill.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The global privacy landscape is constantly changing. Data is regarded as power and even considered as the new commodity; at the same time, data subjects and regulators are increasingly demanding data privacy to avoid personal data violation. This is driving the imminent enactment of a new law in Argentina, in line with the GDPR.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies in the Latin American countries will face the same challenges currently posed by the GDPR in the EU as new data protection laws are introduced.

12.3 What do you envision the privacy landscape will look like in five years?

Expected legislative changes may lead to a different scenario in the upcoming years. It is expected that local law and regulations will be aligned with international standards and the principles established by the GDPR.

AUSTRALIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Australia.

Privacy is regulated in Australia through legislation at both the Federal and State/Territory level.

At the federal level, the Privacy Act 1988 (Cth) ('Privacy Act') regulates the handling of personal information by federal government agencies and private organizations with a turnover of AU\$3 million or more, as well as certain other private organizations regardless of turnover. Private organizations (with a turnover of less than AU\$3 million) are generally not regulated by the Privacy Act (this is known as the 'small business exemption'). Whilst the Australian Government has indicated that it agrees in principle with the 2023 Privacy Act Review Report's proposal to remove the small business exemption subject to further consultation with small business, this was not included in the first tranche of reforms to the Privacy Act introduced by the Privacy and Other Legislation Amendment Act 2024 (Cth) ('Privacy Amendment Act'). When such amendments will be made is presently unclear.

Under the Privacy Act, the regulation of the handling of personal information is primarily addressed by the 13 Australian Privacy Principles ('APP's), which set out minimum standards, rights and obligations around the collection, use, storage and disclosure of personal information (see question 4.1). The Privacy Act also sets out various other obligations in respect of the handling of credit information and tax-file numbers.

The Office of the Australian Information Commissioner ('OAIC') is the independent national regulator for privacy, and is responsible for promoting and enforcing privacy law in Australia.

Most Australian States and Territories have their own privacy legislative or administrative regime which is discussed in further detail below.

1.2 What are the primary laws regulating privacy in Australia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

There are a number of different laws in Australia that regulate privacy:

- (a) At the Federal level:
 - (i) The Privacy Act is the primary piece of legislation that regulates privacy and the handling of personal information (which includes health information).
 - (ii) The Spam Act 2003 (Cth) ('Spam Act') regulates commercial electronic messages; and
 - (iii) The Do Not Call Register Act 2006 (Cth) ('Do Not Call Register Act') deals with the marketing of certain types of marketing communications.
- (b) Most Australian States and Territories have their own legislative system or administrative regime to manage the privacy of individuals. Many apply to health records, and/or information processed in the public sector; however, the scope of the application of these regimes varies significantly between the State and Territory jurisdictions.

There are also specific requirements under banking, insurance, superannuation, health and education legislation. For example, in most Australian States and Territories there are also various other regulatory regimes that have specific privacy requirements, such in relation to specific forms of surveillance, individual's rights to request information from government agencies (known as 'freedom of information' or 'FOI'), and in relation to specific industries such as education.

As a result, some requirements can vary between jurisdictions and industries.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Australia does not have any self-regulatory bodies for privacy matters.

1.4 How is privacy law enforced in Australia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Privacy Act is administered by the OAIC. The OAIC has a number of regulatory powers under the Privacy Act and its preferred regulatory approach is to facilitate voluntary compliance and work with entities to encourage best practice. The OAIC seeks to promote and ensure the protection of personal information, consistent with the objectives of the Privacy Act.

The OAIC Commissioner may also take more serious regulatory action such as undertaking investigations and using its enforcement powers to address any potential breaches of the privacy laws, including (but not limited to):

- (a) accepting an enforceable undertaking,
- (b) making a determination, or
- (c) applying to the court for a civil penalty order for a breach of a penalty provision.

There are various regulatory bodies in the Australian States that respond to complaints relating to health information or management of information by a State government organization or contractor, as well as in specifically regulated industries (such as the Australian Prudential Regulation Authority in relation to banking, insurance and superannuation services).

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Australia?

The APPs under the Privacy Act set out a minimum standard for the handling of personal information, and apply to 'APP entities' which means 'agencies' or 'organizations'.

'Agencies' consist of Australian Federal government agencies and other prescribed federal bodies. An 'organization' includes an individual (including a sole trader), body corporate, partnership, unincorporated association or trust that is not a small business operator (as that term is defined in the Privacy Act), registered political party, agency, State or Territory authority or a prescribed instrumentality of a State or Territory.

2.2 Does privacy law in Australia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the Privacy Act has an extra-territorial application. It applies to the overseas activities of Australian organizations and to foreign organizations that have an 'Australian link'. An organization is considered to have an Australian link if:

- (a) there is an organizational link: eg, the organization is a company incorporated in Australia, or a trust created in Australia; or
- (b) the organization carries on business in Australia or an external territory, and collects or holds personal data in Australia or an external territory.

Whether an organization ‘carries on business in Australia’ is a question of fact, and an assessment should be made having regard to all relevant circumstances, particularly the nature of the enterprise being conducted by the entity concerned.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Australia?

The Privacy Act defines ‘personal information’ as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in material form or not’.

The Australian Government has indicated that it agrees in principle with the 2023 Privacy Act Review Report’s proposal that the definition of personal information should be amended so that information need only ‘relate to’ an individual, and prescribe a non-exclusive list of examples of personal information, including online identifiers (such as IP addresses and device identifiers). Exactly when such amendments will be made is presently unclear.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Privacy Act defines ‘sensitive information’ as:

- (a) information or an opinion about an individual’s:
 - (i) racial or ethnic origin;
 - (ii) political opinions;
 - (iii) membership of a political association;
 - (iv) religious beliefs or affiliation;
 - (v) philosophical beliefs;
 - (vi) membership of a professional or trade association;
 - (vii) membership of a trade union;
 - (viii) sexual orientation or practices; or
 - (ix) criminal record,
 that is also personal information;
- (b) health information about an individual;
- (c) genetic information about an individual that is not otherwise health information;
- (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- (e) biometric templates.

Generally, the handling of ‘sensitive information’ is subject to stricter obligations, and generally requires the consent of the relevant individual or other exceptions at law to apply in regards to its handling.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Whether anonymized, pseudonymized or de-identified data is considered ‘personal information’ and therefore regulated under the Privacy Act is a matter of interpretation. The Privacy Act only applies to information which is about an ‘identified individual, or an individual who is reasonably identifiable’.

However, even if the information does not constitute ‘personal information’ on its own, if it can be connected with other information held by the business (even if it is stored separately), or a related entity, or is reasonably accessible based on the ‘motivated intruder’ test, to the extent that, when connected, it is capable of identifying an individual, then it must be treated as personal information and the Privacy Act and the APPs will apply.

APP 2 requires APP entities to allow individuals the option to remain anonymous or to use a pseudonym when dealing with the APP entity, except where impracticable or a prescribed exception applies.

Further, APP 11 requires an APP entity to take such steps as are reasonable in the circumstances to destroy or de-identify any personal information once it is no longer required for the purpose for which it may be used or disclosed.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

There are 13 APPs contained within the Privacy Act that APP entities need to follow when dealing with personal information. The APPs are summarized in high level below:

- (a) **APP 1—Open and transparent management of personal information:** APP entities are required to take such steps as are reasonable in the circumstances to implement practices and procedures to ensure that the APP entity complies with the APPs and manages personal information in an open and transparent way. This includes having the ability to deal with enquiries and complaints from individuals about the APP entity’s compliance with the APPs and having a clear and up to date organization privacy policy (which must include the prescribed information under APP 1.4).
- (b) **APP 2—Anonymity and pseudonymity:** APP entities must allow individuals the option to remain anonymous or to use a pseudonym when dealing with the APP entity, except where impracticable or a prescribed exception applies.
- (c) **APP 3—Collection of solicited personal information:** APP entities may only solicit and collect personal information where it is reasonably necessary for one or more of the APP entity’s functions or activities or where an exception applies. In addition, APP entities may only solicit and collect personal information which is sensitive information if the individual consents to the sensitive information being collected, unless an exception applies. APP entities must also only collect personal information by lawful and fair means.
- (d) **APP 4—Dealing with unsolicited personal information:** If an APP entity receives unsolicited personal information, it is required to determine whether it would otherwise have grounds on which to collect it. If the APP entity does have such grounds, it may retain the personal information, provided that it complies with the remaining APPs. If the APP entity does not have such grounds, it must destroy or de-identify the personal information.
- (e) **APP 5—Notification of the collection of personal information:** An APP entity that collects personal information about an individual is required to take reasonable steps either to notify the individual of certain matters or to ensure that the individual is aware of those matters. These matters are set out in APP 5.2 and include:
 - (i) the entity’s identity and contact details;
 - (ii) the fact and circumstances of collection;

- (iii) whether the collection is required or authorized by law;
- (iv) the purposes of collection;
- (v) the consequences if personal information is not collected;
- (vi) the company's usual disclosures of personal information of the kind collected by the company;
- (vii) that the entity's APP privacy policy contains information about how the individual may access or seek correction of the personal information that is held about them;
- (viii) how the individual may complain about a breach of the APPs and how the entity will deal with such a complaint; and
- (ix) whether the entity is likely to disclose personal information to overseas recipients, and, if so and if practicable, the countries where they are located.

The notification can be done through a variety of formats, such as over the phone, online or hard copy notice.

- (f) **APP 6—Use or disclosure of personal information:** An APP entity can only use or disclose personal information for a purpose for which it was collected (ie, the primary purpose), unless:
 - (i) the individual has consented to a secondary use or disclosure, or
 - (ii) the individual would reasonably expect their personal information to be used for the secondary purpose, or
 - (iii) another prescribed exception applies (such as that the disclosure is necessary to protect someone's health or safety, or the disclosure or secondary use is required or authorized by or under an Australian law or a court/tribunal order).
- (g) **APP 7—Direct marketing:** An APP entity must not use or disclose personal information it holds for the purpose of direct marketing to an individual unless the individual reasonably expects it, or consents to it, and there is an 'opt out' process in place through which the individual can elect not to receive direct marketing communications. APP 7 does not apply where the Spam Act or Do Not Call Register Act apply.
- (h) **APP 8—Cross-border disclosure of personal information:** Under APP 8.1, an APP entity that discloses personal information to an overseas recipient must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1), unless an exception under APP 8.2 applies. In the absence of an APP 8.2 exception applying, the Privacy Act also deems the APP entity liable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs. See also question 8.1.
- (i) **APP 9—Adoption, use or disclosure of government related identifiers:** APP entities are restricted from adopting, using or disclosing a government-related identifier (ie, a number, letter or symbol, or combination of any of those things, used to identify an individual or verify the identity of an individual, that has been assigned by a government agency, a State or Territory authority, an agent of a government agency or authority, or a contracted service provider for a Commonwealth or State contract) unless an exception under APP 9.2 applies.
- (j) **APP 10—Quality of personal information:** APP entities must take reasonable steps to ensure that the personal information they collect is accurate, up-to-date and complete, and ensure that the personal information they use or disclose is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.
- (k) **APP 11—Security of personal information:** APP entities must take reasonable steps to protect the personal information they hold from misuse, interference, loss, and unauthorized access, modification or disclosure. Once an APP entity no longer needs any personal

information for a purpose for which it may be used or disclosed, then it must also take such steps as are reasonable in the circumstances to destroy or de-identify the information.

- (l) **APP 12—Access to personal information:** APP entities that hold personal information about an individual are required to give the individual access to that information on request, unless an exception applies, and must comply with the applicable obligations in relation to providing such access.
- (m) **APP 13—Correction of personal information:** APP entities are required to take reasonable steps to correct personal information if so requested by the individual to ensure that, having regard to the purpose for which it is held, the personal information is accurate, up-to-date, complete, relevant and not misleading.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

The Privacy Act does not consider distinctions between data controllers and data processors. Any handling of personal information, whether collecting, storing, processing or otherwise, is potentially subject to privacy legislation.

The Australian Government has indicated that it agrees in principle with the 2023 Privacy Act Review Report's proposal to introduce the concepts of controllers and processors into the Privacy Act subject to further consultation with small business. When such amendments will be made is presently unclear.

4.3 **Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

As a general rule, the APPs allow an APP entity to use or disclose personal information for the purpose for which it was collected, and for other purposes ('secondary purpose') if the individual has consented, or the secondary purpose is related (or, in the case of sensitive information, directly related) to the primary purpose and such use or disclosure might reasonably be expected by the individual, or where another exception applies.

5 **TRANSPARENCY AND CONSUMER RIGHTS**

5.1 **What information must companies include in their privacy notices when processing personal data for advertising purposes?**

APP 1 requires an APP entity to have a clearly expressed and up-to-date privacy policy detailing the management of personal information by the APP entity. It must contain the following information:

- (a) the kinds of personal information that the entity collects and holds;
- (b) how the entity collects and holds personal information;
- (c) the purposes for which the entity collects, holds, uses and discloses personal information;
- (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- (e) how an individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- (f) whether the entity is likely to disclose personal information to overseas recipients; and
- (g) if the entity is likely to disclose personal information to overseas recipients, the countries in which such recipients are likely to be located (if it is practicable to specify those countries in the policy).

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) The Australian Government has indicated that it agrees in principle with the 2023 Privacy Act Review Report's proposal that individuals be provided with an unqualified right to opt out of their personal information being used or disclosed for direct marketing purposes. This proposal is expected to be addressed in 'Tranche 2' of the proposed amendments to the Privacy Act, which is expected to occur in the second half of 2025. See also question 5.3 regarding APP 7.
- (b) In any context (advertising or otherwise), individuals have the right, under APP 12, to access their personal information held by an APP entity.
The APP entity must give an individual access to their personal information when it has been requested by the individual, except where the law allows the APP entity to refuse the request. Examples of instances where access can be refused are provided in APP 12.3, and include:
 - (i) the APP entity reasonably believes that giving the individual access may pose a serious threat to the life, health or safety of any individual, or to public health or safety;
 - (ii) giving the individual access would have an unreasonable impact on the privacy of other individuals;
 - (iii) the request is frivolous or vexatious;
 - (iv) the personal information is part of existing or anticipated legal proceedings between the individual and the organization; or
 - (v) where a further exception applies.
- (c) Under APP 13, individuals can request a correction of their personal information an APP entity holds about them if the personal information is inaccurate, out-of-date, incomplete, irrelevant, or misleading.
- (d) Individuals also have the right to access and correct government records which contain an individual's personal information under the Freedom of Information Act 1982, and the right to access and correct police records by contacting the Australian Federal Police or the local criminal records section of the police service.
- (e) An individual may complain to the OAIC about an act or practice that interferes with their privacy. If a complaint is made, the OAIC is required to investigate the act or practice, except in certain circumstances.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

APP 7 provides a general prohibition against direct marketing unless an individual reasonably expects it, or consents to it, and there is an 'opt out' process in place through which the individual can elect not to receive direct marketing communications. However, APP 7 does not apply where the Spam Act or Do Not Call Register Act apply.

The sending of electronic commercial communications (including email and SMS) is regulated by the Spam Act. The Spam Act generally requires such communications to identify the sender, to only be sent with the consent of the recipient, and to include a functional unsubscribe facility. Consent may either be express or inferred. Inferred consent is defined in the Spam Act as 'consent that can reasonably be inferred from the conduct and business and other relationships of the individual or organization concerned.'

In addition, the Do Not Call Register Act generally prohibits the making of unsolicited telemarketing calls to a telephone number registered on the Do Not Call Register, unless the account holder of the telephone number has consented to receiving the call.

As noted above at question 5.2, the Australian Government has indicated that it agrees in principle with the 2023 Privacy Act Review Report's proposal that individuals be provided with an unqualified right to opt out of their personal information being used or disclosed for direct marketing purposes, which is expected to be addressed in 'Tranche 2' of the proposed amendments to the Privacy Act.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

If the advertiser is providing de-identified information to the third party, there is no use or disclosure of personal information by the advertiser and the Privacy Act does not apply.

Any use or disclosure of information about an identified individual, or an individual who is reasonably identifiable (or capable of reidentification), will be subject to the APPs and, where applicable, the Spam Act and Do Not Call Register Act, and so it will be necessary to comply with those requirements. These include the requirement to:

- (a) have a clearly expressed and up-to-date privacy policy which includes the purposes for which personal information is collected, held, used and disclosed (APP 1.4);
- (b) notify individuals of the APP entity's usual disclosures of personal information and whether personal information is likely to be disclosed to overseas recipients (APP 5.2);
- (c) only use or disclose personal information for a purpose for which it was collected or for a secondary purpose if an exception applies (APP 6.1);
- (d) if personal information is disclosed to an overseas recipient, take reasonable steps to ensure that the overseas recipient does not breach the APPs (APP 8.1);
- (e) ensure the personal information it uses or discloses is accurate, up to date, complete and relevant (APP 10.1); and
- (f) take reasonable steps to ensure the security of personal information they hold, including taking steps and implementing strategies in relation to third party providers (APP 11.1).

It is important to note that an entity 'holds' personal information if it has the right or power to deal with it (regardless of whether it has physical possession of the information). For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, 'holds' that personal information for the purposes of the Privacy Act.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

APP entities need to comply with the obligations under the Privacy Act and APPs. Entities may be liable if they disclose personal information to a third party and that third party misuses or mishandles the personal information.

Accordingly, third party contracts should:

- (a) specify the purpose for which the personal information is being supplied to the third party;
- (b) require the third party to comply with the Privacy Act and APPs;
- (c) require the third party to notify the disclosing entity immediately if there is a data breach and to assist the disclosing entity with fulfilling its obligations under the Privacy Act; and
- (d) require the third party to indemnify the disclosing entity for failing to comply with the Privacy Act and APPs.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

APP 11 requires APP entities to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorized access, modification or disclosure. This requires companies to implement robust privacy and security measures throughout the entire lifecycle of personal information handling.

The OAIC recommends that organizations adopt a ‘privacy by design’ approach, ensuring that appropriate privacy practices are integrated into the project planning process. As part of this approach, the OAIC encourages organizations to conduct a Privacy Impact Assessment for any new project that will involve the handling of personal information. It should be conducted early enough in the project’s development to allow for adjustments to the project design, or, if significant negative privacy impacts are identified, to reconsider moving forward with the project.

Importantly, organizations should not adopt a ‘set and forget’ approach. Regular reviews should be carried out to ensure that privacy practices remain effective, appropriate and compliant with privacy obligations.

The OAIC has developed a guide to undertaking privacy impact assessments which is available online.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications via electronic messages (including email and SMS) are regulated by the Spam Act. The Spam Act regulates how electronic messages with an ‘Australian link’ are transmitted. In broad terms, an ‘Australian link’ includes any message that originates in Australia, where the sender is present in Australia or the recipient is in Australia. A ‘commercial electronic message’ (which will capture almost all marketing communications, as this relates to a message where the purpose of the message is to offer, advertise or promote the supply of goods or services) must not be sent without the consent of the recipient, and must otherwise identify and provide the contact details of the sender, and must include a functional unsubscribe facility. Failure to comply with these obligations can result in substantial penalties being imposed on corporations.

The Do Not Call Register Act prohibits unsolicited telemarketing calls made to a telephone number registered on the Do Not Call Register, unless the account holder of the telephone number has consented to receiving the call. The Do Not Call Register is a database where individuals can register their numbers to opt out of most unsolicited telemarketing calls. A business must check its marketing lists against the Do Not Call Register to avoid calling or faxing those numbers. If a business outsources telemarketing calls, both the business and the outsourcing provider are responsible for complying with the Do Not Call Act.

7.2 **How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?**

Use of tracking technologies or cookies are not specifically regulated in Australia, as they are not (without combining them with additional identifying data) considered to be ‘personal information’ as defined under the Privacy Act. Where the identification of an individual is enabled by tracking technologies, the use of those tracking technologies will be subject to the APPs.

Whilst not specifically regulated in Australia, individuals are generally given the option to manage the use of tracking technologies under the options or settings on a browser. Individuals can either block, turn off, accept or decline the use of tracking technologies.

The OAIC provides guidance for private sector organizations that use third-party tracking pixels on their website.

7.3 **How are loyalty programs and promotions regulated under privacy law?**

There are currently no specific laws regulating privacy in respect of loyalty programs and promotions in Australia. If the consumer data has been de-identified, the businesses conducting the loyalty programs or promotions are free to sell insights from such consumer data to third parties without the consumers’ knowledge and consent, which results in targeted advertising by such third parties. Of course, if the information is not de-identified, all of the APPs and applicable obligations under the Privacy Act will apply.

7.4 **How is social media and influencer marketing regulated under privacy law?**

Organizations in Australia that collect personal information via social media platforms are regulated by the Privacy Act in the same way they would be if they collected personal information via any other means. The channel by which personal information is collected may vary, but the principles that apply to the collection, use, storage and disclosure of personal information remain the same.

7.5 **How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

Where advertisers target certain individuals using information which is not about an ‘identified individual, or an individual who is reasonably identifiable’, the Privacy Act does not apply. Online behavioral advertising is conducted by collecting web browsing activities and linking this to certain non-identifying information, such as an IP address, in order to direct targeted ads to web pages visited by the user of that IP address. As such, no personal information is being collected, used or disclosed and therefore, the Privacy Act does not apply.

Similarly, contextual advertising displays advertisements based on the content of the webpage an individual is viewing, rather than utilizing an individual’s data or browsing history. Accordingly, no personal information is being collected, used or disclosed and therefore, the Privacy Act does not apply.

However, it is important to note that, even if the information used by an organization to advertise is not itself ‘personal information’, if it can be linked with other information held by the organization (even if it is stored separately), or a related organization, or is reasonably accessible based on the ‘motivated intruder’ test, to the extent that, when it is linked up, it becomes information about an identifiable individual, then it must be treated as personal information and the Privacy Act will apply. The use of big data by companies highlights this issue, as, the more layers of information that are collected about a user, the easier it becomes to identify the individual, and the question is: at what point does it become personal information?

The Australian Government has indicated that it agrees in principle with the following proposals from the 2023 Privacy Act Review Report:

- (a) targeting individuals should be fair and reasonable in the circumstances;
- (b) targeting individuals based on sensitive information should be prohibited, with an exception for socially beneficial content; and
- (c) requiring APP entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals.

The Australian Government noted the proposal to provide individuals with an unqualified right to opt out of receiving targeted advertising and stated that further consideration will be given to ways to enhance individuals' choice and control over how their information is used for such advertising.

The Australian Best Practice Guideline for Online Behavioral Advertising (also called Australian Best Practice Guidelines for Interest Base Advertising) was developed by Australia's leading business and industry associations in the online advertising sector, and are Australia's first self-regulatory guidelines for third party online behavioral advertising. The guidelines set out self-regulatory principles for online behavioral advertising, and aim to promote transparency and consumer awareness and to encourage best practice and accountability.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not specifically regulated in Australia but must comply with the general principles set out in the Privacy Act and APPs regarding the collection, use, storage and disclosure of personal information (see question 4.1).

The Digital ID Act 2024 and the Digital ID (Transitional and Consequential Provisions) Act 2024 provide strong privacy safeguards when creating and using Digital IDs from accredited providers which operate in addition to the general obligations under the Privacy Act.

Data clean rooms allow organizations to upload their data into a secure environment. The data is then de-identified so that it can be shared with participating organizations for data collaboration and analysis. Once the data has been de-identified, it is no longer personal information and the Privacy Act does not apply. However, even if the information does not constitute personal information on its own, if it can be connected with other information, to the extent that, when connected, it is capable of re-identification, then it must be treated as personal information and the Privacy Act will apply.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not specifically regulated in Australia and is otherwise governed by the general principles set out in the Privacy Act and APPs regarding the collection, use, storage and disclosure of personal information (see question 4.1).

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are considered businesses that 'trade' in personal information, as they collect or disclose an individual's personal information to someone else for a benefit, service or advantage (eg, a payment, concession, subsidy or some other advantage or service). Businesses that trade in personal information are specifically regulated under the Privacy Act and will need to comply with the APPs, even if they are a small business (ie, turnover is less than the threshold AU\$3 million).

7.9 How is advertising to children and minors regulated under privacy law?

The Privacy Act protects an individual's personal information regardless of their age.

Guidance provided by the OAIC indicates that a business must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If it is not practical to do so, a business may assume an individual over the age of 15 has capacity to consent, unless there is something to indicate otherwise.

The Privacy Amendment Act requires the OAIC to develop a Children's Online Privacy Code by 10 December 2026 which should set out how the APPs are to be applied or complied with in relation to the privacy of children.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The Privacy Act and APPs apply to all use of artificial intelligence ('AI') involving personal information. Personal information includes inferred, false or AI-generated information (eg, deepfakes and hallucinations) about an identified individual, or an individual who is reasonably identifiable.

The OAIC provides guidance on privacy and the use of commercially available AI products on their website.

From 10 December 2026, if an APP entity uses a computer program to make a decision, the decision could reasonably be expected to significantly affect the rights of interests of an individual, and the computer program uses an individual's personal information to make the decision, then the APP entity's privacy policy must include information regarding the kinds of personal information used by the computer program, and the kinds of decisions made by the computer program.

7.11 Are there other specific advertising practices that you wish to discuss?

The use of biometric data in advertising is still in its early stages in Australia but is becoming a growing focus for regulators, especially given its potential to infringe on privacy.

Under the Privacy Act, biometric data is classified as sensitive information. This means that use of biometric data for advertising (such as facial recognition, emotion detection and voice analysis) requires the consent of the individual before it can be collected or used.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Personal information can be transferred to an overseas office of the same APP entity without the transfer constituting a 'disclosure'. However, transfers to a related body corporate located outside of Australia will constitute a 'disclosure' as the related body corporate is a different entity to the APP entity.

Cross-border disclosure of personal information is regulated under APP 8. Before an APP entity discloses personal information to a person located outside of Australia, the APP entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information unless an exception under APP 8.2 applies, namely if:

- (a) the APP entity reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that, overall, is substantial similarity to the APPs and the individual can take action to enforce such protections;
- (b) APP 8.3 applies to the disclosure (APP 8.3 was inserted by the Privacy Amendment Act, and introduces a whitelist mechanism to allow for disclosure of personal information to prescribed countries with substantially similar privacy protections. To date, no official whitelist has been introduced.);
- (c) the entity has obtained the individual's consent to the foreign disclosure;
- (d) the foreign disclosure is required or authorized by Australian law;
- (e) such disclosure is required by a government agency under an agreement to which Australia is a party;
- (f) the disclosure is by a government agency and relates to foreign law-enforcement activities; or
- (g) a permitted general situation applies (such as to prevent serious health and safety risks).

Where a cross-border disclosure is made to an overseas recipient under APP 8.1, then any act or practice engaged in by the overseas recipient is taken to have been done or engaged in by the APP entity and the APP entity will consequently be held liable for any breach of the APPs by the overseas recipient as if it has done such act itself.

Australia does not have a 'blacklist' of countries where transfers of personal information are prohibited.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The collection or disclosure of personal information (other than sensitive information) from an organization to a related body corporate is not taken to be an interference with the privacy of an individual for the purposes of the Privacy Act. Therefore, collections and disclosures can be made in circumstances that might not otherwise be permissible under the APPs. However, the Privacy Act requires that in holding or using the personal information, they comply with the APPs in relation to the personal information.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Australia? Are there minimum standards? Does this differ by sector or size of the entity?

Under APP 11, APP entities must take such steps as are reasonable in the circumstances to protect the personal information they hold from misuse, interference, loss, unauthorized access, modification or disclosure. The 'reasonable steps' that an APP entity should take will depend on the relevant circumstances, including the relative size and complexity of the business, the sensitivity of the information held, the possible adverse consequences for an individual in the case of a breach and the practical implications in implementing the security measures. Reasonable steps could include internal training, ICT security, access security, physical security and the destruction and de-identification of data when no longer required.

The OAIC advocates for prevention of data breaches where possible through promoting information security. The OAIC has produced a guide to securing personal information, and, whilst not binding, this guide will be referred to by the OAIC when exercising regulatory powers in response to a breach, complaint or non-compliance. The guide is available on its website.

9.2 **How are personal data breaches regulated in Australia? What are the requirements for notification and response?**

Part IIIC of the Privacy Act sets out the obligations in relation to the notification of eligible data breaches. Those entities concerned are required to notify affected individuals and the OAIC about 'eligible data breaches'.

An 'eligible data breach' occurs where there is unauthorized access to, unauthorized disclosure of, or loss of personal information held by an entity and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates, which risk cannot be addressed by remedial action on the part of the entity before any such harm arises.

Determining whether 'serious harm' is likely as a result of the breach involves deciding whether a reasonable person in the position of the entity would consider that a data breach would likely result in serious harm to an individual whose information was involved in the breach. If there is no likelihood of serious harm (despite any unauthorized access, disclosure or loss of personal information), then an incident will not be an eligible data breach and no notification obligation arises.

If an entity only has reason to suspect (but not believe) it has suffered an eligible data breach, then it has an obligation to conduct a reasonable and expeditious investigation into the incident (which should be completed within 30 days).

Once an entity has grounds to believe it has suffered an eligible data breach (which could be at any time, including upon becoming aware of the incident or during the investigation of an incident), then the entity has an obligation to notify the OAIC and the affected individuals. Generally, this notification requires the completion of a prescribed form which largely describes the incident to the OAIC and notifying individuals of the content of such form.

The OAIC provides a guideline for suggested steps if a data breach is suspected:

- (a) Contain the breach: Take immediate steps to limit further access or distribution of the information.
- (b) Assess whether the breach is likely to result in serious harm. Consider whether remediation is possible.
- (c) If serious harm is likely and it is deemed to be an 'eligible data breach', prepare a statement to the OAIC containing the entity's contact details, description of the breach, nature of the information and recommended steps for individuals.
- (d) Following notification to the OAIC, notify affected individuals. The entity may notify all individuals, only those at risk of serious harm, or, if neither of those options is reasonably practicable, publish a statement on the entity's website and publicize it.
- (e) Finally, a review of the incident should be conducted and consideration should be given to what actions can be taken to prevent future breaches.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The Privacy Act confers a range of regulatory powers on the Commissioner, including investigation and enforcement powers, which are based on an escalation model. This includes powers to conciliate complaints, to make preliminary enquiries of any person, to require the provision of information or documents and to make determinations in relation to an investigation.

The preferred regulatory approach of the OAIC is to work with entities to facilitate legal and best practice compliance. For example, engaging with regulated entities to provide guidance, promote best practice compliance, and identify and seek to address privacy concerns as they arise.

An investigation may be commenced by the OAIC into a suspected or alleged interference with privacy, either on receipt of a complaint or as a Commissioner-initiated investigation ('CII'). Following a complaint investigation or CII, the Commissioner may make a determination about the particular conduct and decide to take enforcement action against an entity.

Under the Privacy Act, enforcement powers range from less serious to more serious regulatory action, and include powers to:

- (a) accept or enforce an enforceable undertaking;
- (b) make a declaration that the complainant is entitled to a specific amount by way of compensation for any loss or damage suffered;
- (c) make a determination or bring proceedings to enforce a determination;
- (d) seek an injunction to prevent a potential privacy breach from continuing; or
- (e) apply to the court for a civil penalty.

The OAIC may apply to the Federal Court or Federal Circuit Court for an order that the entity pay the Commonwealth a penalty. The maximum penalty for a serious interference with privacy by an entity is an amount not exceeding the greater of AU\$50 million or three times the value of the benefit obtained directly or indirectly by the body corporate and any related bodies corporate, that is reasonably attributable to the conduct constituting the contravention; or, if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention.

10.2 Do consumers have a private right of action? What remedies are available to them?

(a) Common law rights

The possibility of a tort of privacy has historically been left open by superior courts, mostly notable by the High Court in 2001 in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*. However, in the recent 2024 decision of *Lynn Waller (pseudonym) v Romy Barrett (pseudonym)*, the County Court of Victoria awarded damages to the plaintiff to compensate for a serious invasion of privacy. While the decision is yet to be approved by a superior court, it represents a clear judicial recognition of a cause of action for serious invasions of privacy.

(b) Statutory rights

The Privacy Amendment Act introduces Schedule 2 which establishes a cause of action in tort for serious invasions of privacy. Schedule 2 will take effect on 10 June 2025, unless an earlier date is fixed by proclamation. Under Schedule 2, an individual has a cause of action in tort against another person if, among other things, the other person invaded the individual's privacy by intruding upon their seclusion or misusing information relating to them.

It is a defense if the defendant acted with lawful authority or in certain circumstances involving consent, necessity or the defense of persons or property. If the defendant published information about the plaintiff, the defendant may also have access to certain defenses that would ordinarily arise in the context of defamation proceedings.

The remedies available include damages, an account of profits, an injunction, a declaration, an order requiring the defendant to apologize, a correction order, and an order requiring any relevant material to be destroyed, delivered up or dealt with as the court directs.

The sum of damages for non-economic loss and any exemplary or punitive damages must not exceed the greater of AU\$478,550 and the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The recent amendments to the Privacy Act provide the OAIC with expanded enforcement and investigation powers.

The OAIC has been increasingly active in taking regulatory action and finalized 15% more Information Commissioner reviews and 20% more privacy complaints in 2023-24 than in previous years.

On 17 December 2024, the OAIC accepted an enforceable undertaking from Meta Platforms, Inc. ('Meta'). Meta agreed to pay AU\$50 million on a without prejudice and without admissions basis to resolve civil penalty proceedings which had been commenced by the OAIC for alleged breaches of the Privacy Act in relation to the Cambridge Analytica incident. The incident involved Meta releasing the personal information of millions of Facebook users globally (including over 311,000 Australians) which was provided to Cambridge Analytica and purportedly used for political advertising during the 2016 US presidential election. The case is a landmark settlement and represents the largest payment relating to individual privacy concerns in Australia. The sum is intended to compensate eligible Australians affected by the incident.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Australia?

There is currently no privacy-related legislation in Australia which is specific to Australian culture. However, there are cultural protocols about how certain Aboriginal and Torres Strait Islander individuals may be portrayed in various types of media. These rules, whilst focused on spiritual and cultural sensitivities, may also protect an indigenous person's sense of privacy. For example, the reproduction of a deceased person's name and image is offensive to some indigenous cultural beliefs. It is recommended that cultural warnings are used at the beginning of any audio-visual media to alert Aboriginal and Torres Strait Islander viewers and/or listeners that images and/or voices of deceased persons may be used. It is also generally recommended that any depictions of Aboriginal people be reviewed by an appropriate indigenous arts body to confirm that such depictions are culturally sensitive and accord with Aboriginal religious and cultural beliefs and are not offensive to or misrepresents their laws and customs.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

The Privacy Amendment Act amended APP 11 to provide that 'reasonable steps' in relation to the security of personal information now include both technical and organizational measures. The amendments emphasize the expectation that organizations must have sufficient practices, policies and procedures to ensure cybersecurity and protect against data breaches. Organizations should take clear, demonstrable steps to ensure staff understand their privacy obligations, and there are systems in place to protect personal information.

The OAIC's shift towards becoming a more enforcement-focused regulator highlights the need for organizations to adopt proactive privacy practices, including regular audits and a well-prepared data breach response plan.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Where handling sensitive information, there are greater obligations to that must be complied with, including, but not limited to ensuring that individuals are aware:

- (a) that their personal information is being collected,
- (b) of the purposes for which the information is collected, and
- (c) that consent is obtained for the use or disclosure of the information.

If personal information about Australian individuals is stored overseas it is still regulated under Australian privacy law. Care should be taken when outsourcing the storage of personal data, for example, through cloud hosting services.

The Privacy Act also sets out other obligations in respect of 'credit information' and 'tax file number information'. In general terms, 'credit information' refers to any personal information that relates to consumer credit taken out by an individual. Further guidance should be sought where dealing with these types of information.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Following the release of the Privacy Act Review Report in February 2023, and the Australian Government's response in September 2023, the Australian privacy law landscape is undergoing significant change, with reforms being implemented in multiple phases.

The Privacy Amendment Act introduced the first tranche of reforms, which include:

- (a) the introduction of a statutory tort for serious invasions of privacy;
- (b) the introduction of a criminal offence of 'doxxing';
- (c) expansion of the civil penalty regime;
- (d) enhanced enforcement powers for the OAIC;
- (e) the requirement for the OAIC to develop a Children's Online Privacy Code;
- (f) the requirement for organizations to update their privacy policies to disclose when decisions are made using automated processes;
- (g) introduction of a 'whitelist' mechanism for overseas data transfers; and
- (h) clarification on steps required to protect personal information.

Tranche 2 is expected to occur after May 2025 and cover a broader range of issues, including amendments to the definitions of personal information and consent, introduce a ‘fair and reasonable test’ for information handling and potentially remove the small business exemption. The exact timing and scope are yet to be determined.

Tranche 1 and Tranche 2 are considered the most significant changes to Australian privacy law since the introduction of the APPs in 2014.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Privacy laws have had to evolve to keep up with the ever-changing world of online technology and advanced breaches in data security. Recent changes to the Privacy Act and ongoing reforms mean that companies will need to work harder to ensure compliance with the updated privacy laws. With harsher penalties and expanded enforcement powers now in place, companies are being forced to re-evaluate their privacy policies and processes. As privacy becomes an increasingly crucial priority, this area will likely be of greater focus for a number of years to come.

In the wake of serious data breaches and evolving regulatory expectations, companies are also having to consider new software and technology to increase their data security and protect the personal information they hold. This results in additional compliance costs, as well as ongoing investment to meet the new requirements set out by the privacy reforms.

12.3 What do you envision the privacy landscape will look like in five years?

We anticipate that the Australian privacy landscape will become increasingly regulated in order to bring Australia in line with other countries’ privacy standards, such as Europe, and facilitate global data sharing.

We would expect the next five years would see the implementation of the second and third tranches of the Privacy Act reforms, which will further strengthen Australia’s privacy laws and introduce stricter requirements regarding data collection and handling.

In addition, the first tranche of reforms saw the introduction of a three-tiered civil penalty regime and enhanced regulatory powers, which is likely to lead to a more proactive and enforcement-focused approach by the OAIC. These changes will place greater responsibility on organizations to ensure compliance and adopt stronger data protection measures.

Further, the recent introduction of the Cyber Security Act 2024, following the release of the 2023–2030 Australian Cyber Security Strategy, will enforce stricter data security standards and will influence how businesses manage data breaches and adhere to data minimization practices to protect personal information against unauthorized access and misuse.

 BELIZE 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Belize.

Belize has made strides in its regulation of privacy by virtue of the enactment of the Data Protection Act 2021, the Cybercrime Act 2020 and the Public Sector Data Sharing Act 2021. Privacy is also expressly considered in the Belize Constitution. Furthermore, references to privacy can be found in some laws regulating public and private entities which are required to obtain personal information.

1.2 What are the primary laws regulating privacy in Belize? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The key laws regulating aspects of privacy (including confidential information and confidential data) in Belize are:

- (a) The Belize Constitution Act;
- (b) Interception of Communications Act 2020;
- (c) Cybercrime Act 2020;
- (d) Data Protection Act 2021;
- (e) Public Sector Data Sharing Act 2021; and
- (f) Electronic Transfer of Funds Crime Act 2021.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Data Protection Act establishes that a data subject may, by written notice to a data controller, require the data controller at the end of a 21-day period to cease processing personal data of the data subject for the purposes of direct marketing. A data controller has the responsibility to self-regulate by creating mechanisms to receive this written notice from data subjects and to stop using personal data for unwanted marketing communications. As to direct marketing see question 7.1.

Aside from this, self-regulation plays a limited role in privacy practices related to advertising. The Belize Advertising Standards Authority ('BASA') promotes responsible practices and adherence to ethical standards of honesty, decency, and fairness, and businesses may adopt internal privacy policies and advertising codes that go beyond BASA's requirements and guidance.

1.4 How is privacy law enforced in Belize? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The enforcement of privacy law falls under the jurisdiction of the Belizean judicial system.

The enactment of the Data Protection Act 2021 established the Data Protection Tribunal which has the jurisdiction to adjudicate over matters concerning the use of personal data. Additionally, the Data Protection Act 2021 mandates that there be a Data Protection Commissioner whose responsibilities include providing information to individuals about their rights under the Act, as well as monitoring the processing of personal data and any other matter affecting the privacy of persons in respect of their personal data.

Similarly, the Public Sector Data Sharing Act established the Office for Data Analytics within the Ministry responsible for digital transformation, e-governance and information technology.

There are also regulating bodies within specific industries that utilize personal information to fulfil their duties. For example, the Public Utilities Committee, which regulates the telecommunication sector of Belize and the use of data within that sector, and the Central Bank of Belize, which regulates the banking and finance sector.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Belize?

Privacy laws in Belize are applicable to both the public and private sectors. Notably, small businesses (ie, those whose annual turnover is BZD 3M (approx USD 1.5M) or less) are exempted from the application of the Data Protection Act, save and except for any small business that:

- (a) provides health services;
- (b) trades in personal information;
- (c) is an operator of a residential tenancy database;
- (d) is a credit reporting body;
- (e) is a reporting entity for the purposes of the Money Laundering and Terrorism (Prevention) Act;
- (f) is an employee association registered or recognized under any enactment in Belize;
- (g) is a business prescribed by, under regulations made under the Data Protection Act; or
- (h) is a business that has opted in to be covered by the Data Protection Act.

2.2 Does privacy law in Belize apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Data Protection Act 2021 applies to companies or persons processing personal data as data controllers or data processors established in Belize, as well as those outside of Belize, processing the personal data of data subjects in Belize in relation to the offer of goods or services to data subjects in Belize.

A data controller or data processor is established in Belize if that data controller or data processor is a body, association or other entity incorporated, organized, registered or otherwise formed under the laws of Belize.

The Cybercrime Act stipulates that the courts in Belize have jurisdiction where, among other situations, a regulated act is carried out which affects a computer system located in Belize, or computer data on a computer data storage medium located in Belize is affected by the act, or the effect of the act, or the damage resulting from the act, occurs within Belize.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Belize?

According to the Data Protection Act, ‘personal data’ means data which relates to an individual who can be identified from:

- (a) that data; or
- (b) that data together with other information which is in the possession of, or is likely to come into the possession of, the data controller.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

- (a) The Data Protection Act states that the following categories of personal data are to be considered sensitive:
- (i) racial or ethnic origin;
 - (ii) political opinions;
 - (iii) religious beliefs or other beliefs of a similar nature;
 - (iv) membership of a political body;
 - (v) membership of a trade union;
 - (vi) genetic data;
 - (vii) biometric data;
 - (viii) sexual orientation or sexual life;
 - (ix) financial record or position;
 - (x) criminal record; or
 - (xi) proceedings for any offence committed or alleged to have been committed by a person, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings.

The processing of sensitive personal data is prohibited, subject to certain exceptions, including where:

- the individual consented to their sensitive personal data being processed;
- the processing is necessary to carry out a legal right or obligation; or
- the processing is necessary for the administration of justice.

- (b) Additionally, under the Public Sector Data Sharing Act, ‘confidential or commercially sensitive information’ means:
- (i) information a person controls that the person is required to keep confidential under a contractual or equitable obligation;
 - (ii) without limiting (i) above, information about commercial-in-confidence provisions of contract; or
 - (iii) any other information, the disclosure of which would prejudice any person’s legitimate business, commercial, professional or financial interests.

It should therefore be noted that a data recipient who is provided with public sector data that contains confidential or commercially sensitive information must ensure that the information is dealt with in a way that complies with any prior contractual obligations.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized data which has been irreversibly stripped of identifiers can be utilized without implications under the Data Protection Act’s obligations, as it is not considered ‘personal data’.

De-identified data may, however, trigger the Act’s provisions, depending on how robust the de-identification process is. If re-identification is possible, the Act’s provisions apply, and appropriate measures must be taken to properly handle the data to avoid violating the Act’s provisions. If re-identification is not possible, then the data may be treated like anonymized data and will not engage the Act.

Pseudonymization is expressly contemplated by the Act as an appropriate technical and organizational measure to ensure a level of risk-appropriate security for personal data. Even when personal data is

pseudonymized, it remains personal data, and must be handled in accordance with the Data Protection Act.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) According to the Data Protection Act, personal data should be:
 - (i) processed lawfully, fairly and in a transparent manner in relation to the data subject;
 - (ii) collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes;
 - (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - (iv) accurate and, where necessary, kept up to date and reasonable steps shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
 - (vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
- (b) Additionally, most companies (especially in the tourism industry and banking industries) that are exposed to handling information of EU citizens are implementing the principles set forth in the EU GDPR, namely:
 - (i) lawfulness, fairness and transparency,
 - (ii) purpose limitation,
 - (iii) accuracy,
 - (iv) data minimization,
 - (v) integrity and confidentiality and
 - (vi) storage limitation.
- (c) On another note, the Public Sector Data Sharing Act stipulates that every data provider must abide by the trusted principles of accessing data by first determining:
 - (i) the purpose for which the data is to be shared and used;
 - (ii) whether the data recipient is an appropriate public sector agency; and
 - (iii) whether the results of data analytics work are appropriate for disclosure or publication.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Specific roles based on data processing activities are created under the Data Protection Act. These roles directly shape their legal responsibilities and compliance obligations:

- (a) According to the Data Protection Act, a data controller is a person who determines the purposes for, and the manner in which, any personal data is processed; or the person on whom the obligation to process the data is imposed by or under an enactment.

A data controller is responsible for:

- (i) implementing the appropriate technical and organizational measures to ensure that processing is performed in accordance with the Act;
 - (ii) ensuring lawful data processing;
 - (ii) responding to data subjects' requests for data access, correction or erasure;
 - (iv) conducting data protection impact assessments; and
 - (v) maintaining records of data processing activities..
- (b) A data processor is 'any person, other than an employee of a data controller, who processes personal data on behalf of the data controller'.
- A data processor is required to comply with obligations equivalent to those imposed on a data controller by the Act, including:
- (i) implementing data security measures; and
 - (ii) cooperating with audits and investigations.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Data processing is lawful where data subjects consent to the processing of their personal data for one or more specific purposes. 'Consent' in relation to a data subject means 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him'. It should be noted that data subjects have the right to withdraw consent in respect of the processing of their personal data at any time.

The processing of a child's personal data is lawful only where, and to the extent that, consent is given or authorized by:

- (a) the parent or guardian of the child; or
- (b) the child where the child is over the age of 13.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Privacy notices must be clear and comprehensive. They must include:

- (a) name and contact details of the data controller;
- (b) purpose for processing;
- (c) who might have access to personal data;
- (d) retention period; and
- (e) data subjects' right to access, correct, or erase data and object to data's processing for direct marketing purposes.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) According to current legislation, individuals have the right for their personal information that has been collected from the public sector to remain confidential. Such personal information is only to be shared with that person's written consent, or the consent of their relatives if the person is deceased.

- (b) The Belize Constitution Act provides that, subject to respect for the rights and freedoms of others and for the public interest, every person in Belize is entitled to the fundamental rights and freedoms of the individual, which include protection for their family life, personal privacy, the privacy of their home and other property and recognition of human dignity.
- (c) The Data Protection Act provides that data subjects have the following rights:
 - (i) the right to be informed by a data controller whether personal data of that data subject is being processed by or on behalf of the data controller; or
 - (ii) where personal data of the data subject is being processed by or on behalf of the data controller, the right to request from, and to be given by, the data controller, a description of:
 - the purposes of the processing;
 - the categories of personal data concerned;
 - the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in other countries or international organizations;
 - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - the right to lodge a complaint with the Commissioner;
 - any available information as to their source, where the personal data is not collected from the data subject; or
 - the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
 - (iii) the right to receive a copy of the data undergoing processing,
 - (iv) the right to obtain from a data controller, without undue delay, the rectification of inaccurate personal data concerning the data subject.
 - (v) the right to erasure of personal data without undue delay;
 - (vi) the right to restrict the processing of personal data in specific circumstances;
 - (vii) the right to data portability;
 - (viii) the right to prevent processing that is likely to cause damage or distress;
 - (ix) the right to prevent processing for purposes of direct marketing; and
 - (x) the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on the data subject.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

In Belize, companies must obtain freely given, specific, informed and unambiguous consent from data subjects or provide opt-out mechanisms for direct marketing and targeted advertising.

To meet legal standards, companies must:

- (a) **document consent:** keep records of when and how consent was obtained;

- (b) **use plain language:** privacy notices and consent forms must be easy to understand;
- (c) **enable withdrawal:** users must be able to revoke consent at any time, with no penalty;
- (d) **minimize data use:** only collect data necessary for the stated advertising purpose; and
- (e) **secure data:** implement safeguards to prevent unauthorized access or misuse.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Data controllers are required to make readily available to data subjects:

- (a) the identity of the data controller;
- (b) the purpose for which the data is intended to be processed; and
- (c) any further information which is necessary to enable the processing to be fair.

When third parties are used for advertising data controllers must:

- disclose vendor involvement in privacy notices;
- obtain valid consent if vendors use data for profiling or behavioral targeting;
- ensure opt-out mechanisms are honored across platforms; and
- limit data sharing to what's necessary for the advertising purpose

Where cross-border transfer of personal data will occur, data controllers must ensure that the recipient country has adequate protection standards.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When disclosing or receiving personal data:

- (a) the purpose for which data is shared must be clearly defined and adhered to;
- (b) data must be processed only on documented instructions;
- (c) appropriate technical and organizational safeguards must be in place;
- (d) sub-processors should not be engaged without approval of data controllers;
- (e) breach notification must occur within 72 hours;
- (f) cooperation with audits and inspections must occur;
- (g) contract clauses must ensure adequate data protection for cross-border transfers; and
- (h) upon contract termination, data must be returned or securely deleted.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

- (a) Firstly, pursuant to the Data Protection Act, a data controller and a data processor, and where applicable, their representatives, are expected to maintain a record of processing activities under their purview.
- (b) The Data Protection Act mandates that a data privacy officer is designated where:
 - (i) data processing is carried out by a public body, except when carried out by a court of competent jurisdiction acting in their judicial capacity;
 - (ii) the processing is of such a nature that it requires regular and systematic monitoring of data subjects on a large scale; or
 - (iii) there is large-scale processing of sensitive personal data.

It is the duty of the data privacy officer to cooperate with the Commissioner to ensure that data controllers and data processors comply with the Act.

- (c) Additionally, where a type of processing, in particular processing using new technologies, is likely to result in a high risk to the rights and freedoms of an individual, a data controller must, prior to the processing, carry out a data protection impact assessment of the impact of the envisaged processing operations on the protection of personal data. This assessment should contain:
- (i) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
 - (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
 - (iii) an assessment of the risks to the rights and freedoms of data subjects; and
 - (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The data controller should seek the advice of a data privacy officer when carrying out a data protection impact assessment.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Data controllers must obtain freely given, specific, informed, and unambiguous consent before using personal data for direct marketing. ‘Direct marketing’ means the communication, by any means, of any advertising or marketing material which is directed to particular individuals.

Privacy notices must state that data will be used for marketing, identify recipients, and explain profiling or targeting practices. Data subjects must be able to object at any time to the use of their data for direct marketing, and such objections must be honored without delay.

If marketing involves profiling or automated targeting, this must be disclosed and opt-out options must be offered. Marketing to minors under 16 requires verifiable parental consent, and use of sensitive data such as health, financial, or biometric data, for marketing demands heightened safeguards.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies must be used with express consent and transparency. Users must be clearly informed about what tracking tools are used, what data is collected, and how the data will be used, and users must be able to reject or disable these technologies.

7.3 How are loyalty programs and promotions regulated under privacy law?

Express, informed consent must be given prior to the collection of personal data; there must be sufficient transparency on how data will be used, and participants in loyalty programs and promotions must be able to opt out of marketing communications or data sharing without losing access to the program’s core benefits.

If offers are personalized using behavioral data, companies must disclose this and allow users to opt out. Any sharing of data with ad platforms or analytics firms must be covered by data processing agreements and disclosed in privacy notices.

7.4 How is social media and influencer marketing regulated under privacy law?

- (a) Influencers and brands must obtain express, informed consent before collecting or using personal data for marketing.
- (b) Sponsored content must clearly disclose brand relationships using hashtags like #ad or #sponsored.
- (c) If influencers use behavioral data to personalize promotions, they must explain how profiling works and offer opt-out options.
- (d) Marketing to users under 16 requires verifiable parental consent, especially on platforms like TikTok or Instagram.
- (e) Data shared with ad platforms or analytics vendors must be covered by data processing agreements and disclosed in privacy notices.
- (f) Misleading claims, exaggerations, or unverified endorsements must be avoided; and BASA encourages voluntary compliance with ethical codes and standards in influencer marketing.
- (g) Promotions involving health, financial, or environmental products must be backed by evidence and comply with sector-specific rules.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising is heavily regulated as a result of its use of personal data to deliver personalized ads. Belizean law treats this as high-risk processing, subject to strict requirements of consent, transparency, opt-out rights, and disclosure.

Contextual advertising, however, delivers ads based on non-personal factors without tracking or profiling individuals. Typically, consent is not required and there are minimal disclosure requirements with contextual advertising, as long as personal data is not being collected.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

These are not expressly regulated by the Data Protection Act.

7.7 How is location-based advertising regulated under privacy law?

- (a) Express consent must be obtained prior to collecting and utilizing location data for advertising;
- (b) Privacy notices must explain how location data is collected, what it's used for, and with whom it's shared;
- (c) Users must be able to disable location tracking or opt out of location-based ads at any time;
- (d) Location data must be protected against unauthorized access, misuse, or breaches; and
- (e) Only the minimum necessary location data should be collected for the intended advertising purpose.

7.8 How are data brokers defined and regulated under privacy law?

Under the Data Protection Act, the term 'data broker' is not defined, but the Act effectively regulates data broker activities through its provisions on data controllers, processors, and entities that trade in personal information.

7.9 How is advertising to children and minors regulated under privacy law?

The Data Protection Act prioritizes transparency, parental control, and responsible data use when marketing to persons under 16. Companies must obtain explicit consent from a parent or guardian before collecting or using a child's personal data for advertising.

There must be:

- (a) **No manipulative messaging:** Ads must avoid exploiting children's vulnerability or lack of experience;
- (b) **Age-appropriate content:** Promotions must be suitable for the child's age and maturity level;
- (c) **Disclosure of sponsorships:** Influencer or social media marketing targeting children must clearly identify paid partnerships; and
- (d) **No behavioral tracking without consent:** Cookies or tracking technologies used to target children require verifiable parental consent.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The Data Protection Act takes a cautious and rights-based approach to regulating profiling, artificial intelligence ('AI'), and automated decision-making ('ADM') in advertising. It establishes that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless:

- (a) necessary for entering into, or performance of, a contract between the data subject and a data controller;
- (b) authorized by any enactment to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- (c) based on the data subject's consent.

Profiling requires consent, transparency and opt-out rights. ADM decisions are not to be made without users being informed that the decisions are ADM, and users must be given the right to object. Accountability, fairness and security must be ensured where AI systems are used.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

- (a) Part IV of the Data Protection Act concerns the transfer of personal data outside of Belize. Where personal data is transferred to a country or territory outside Belize, the transferor must ensure there is:
 - (i) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and
 - (ii) appropriate safeguards to ensure that the rights of the data subject are enforceable and that there are effective legal remedies available for data subjects.

In addition, the Act stipulates that a code of conduct or certification mechanism be implemented and that binding corporate rules be developed and submitted to the Commissioner.

- (b) Likewise, under the Public Sector Data Sharing Act, to transfer data between companies or public agencies, the data provider must determine:
 - (i) the purpose for which the data is to be shared and used;
 - (ii) whether the data recipient is an appropriate public sector agency; and
 - (iii) whether the results of data analytics work is appropriate for disclosure or publication.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Transfers may be allowed without consent if necessary for important public interest in Belize. The Data Protection Act provides for the exemption of personal data that enjoy parliamentary or legal privilege. Moreover, privilege between different professionals and individuals is expected, and exists within specific professions, through the Medical Practitioners' Act, the Freedom of Information Act and the Code of Judicial Conduct and Etiquette, among others.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Belize? Are there minimum standards? Does this differ by sector or size of the entity?

- (a) Data security is regulated specifically by the Data Protection Act 2021. This Act is generally applicable once personal data is being processed. Therefore, companies are advised to thoroughly read the Act to ensure that they are operating in accordance with it. Data controllers and processors are required to, among other things:
 - (i) develop binding rules for the transfer of personal data;
 - (ii) apply principles regarding purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of sensitive personal data, and measures to ensure data security; and
 - (iii) establish inter or cross group mechanisms (within a group of enterprises engaged in a joint economic activity) for ensuring the verification of compliance with the binding corporate rules.
- (b) Additionally, Part III of the Interception of Communications Act is especially applicable in cases of wire-tapping and other means of data gathering to investigate criminal offences. It stipulates the sanctions for acquiring protected information or traffic data by means of a communication network for personal use, commercial benefit, political advantage, or criminal activity.
- (c) Furthermore, the Public Sector Data Sharing Act facilitates the sharing of data between public sector agencies and other entities.

9.2 How are personal data breaches regulated in Belize? What are the requirements for notification and response?

- (a) Data breaches are regulated by the Data Protection Act 2021. They are defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized

disclosure of, or access to, personal data transmitted, stored or otherwise processed'. Under this Act:

- (i) a data controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Commissioner of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual;
 - (ii) a data processor must, without undue delay, notify the data controller of a personal data breach, after becoming aware of a personal data breach; and
 - (iii) where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, a data controller must notify the data subject of the personal data breach without undue delay and, where feasible, not later than 70 hours after having become aware of it.
- (b) Data breaches are also regulated by the Interception of Communications Act 2020, wherein they are referred to as 'unauthorized interceptions'. Pursuant to this Act, a person who intentionally intercepts or otherwise acquires protected data or traffic data by means of a communication network commits an offence and is liable to be fined and/or imprisoned.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) A data controller or data processor who fails to comply with the data processing principles outlined in the Data Protection Act commits an offence and is liable on summary conviction to a fine of BZD 500,000 (approx USD 250,000) and/or imprisonment for 3 years.
- (b) A person who fails to comply with the Data Protection Act's requirements when transferring personal data outside of Belize is liable on summary conviction to a fine of BZD 20,000 (approx USD 10,000).
- (c) Furthermore, a data processor who unnecessarily processes data without the instructions of a data controller is liable on summary conviction to a fine of BZD 20,000. This penalty is also applicable to any person who fails to keep secret all confidential information coming to their knowledge during the course of the administration of the Data Protection Act or any other Act that the Commissioner has jurisdiction to administer or enforce.
- (d) A person who knowingly or recklessly, without the consent of a data controller:
 - (i) obtains or discloses personal data or the information contained in personal data; or
 - (ii) procures the disclosure to another person of the information contained in personal data,
 is liable on summary conviction to a fine of BZD 10,000 (approx USD 5,000).
- (e) Moreover, a person who contravenes the Cybercrime Act and/or the Electronic Transfer of Funds Act by misusing the personal or financial data of another person, commits an offence and is liable to be fined and/or imprisoned.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under the Data Protection Act, individuals have the right to lodge complaints with the Commissioner who will then launch investigations and make further decisions accordingly. However, individuals have a private right of action under constitutional law, torts and contract law. The potential remedies are damages.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In the 2024 case of *Belize Sugar Industries Ltd v Attorney General*, the Belizean government required the disclosure of contracts under the Sugar Industry (License to Import/Export Sugar) Regulations 2023. The sugar industry argued that such disclosures would be a breach of informational privacy. It was held that certain aspects of the Regulations were unconstitutional and that legal entities also have privacy rights under the Belizean Constitution. In October 2024, a proposed partnership with a facial recognition software company was placed on hold by Belize’s Police Department citing data privacy concerns.

The Data Protection Commissioner, who is responsible for the general administration of the Act:

- (a) conducts audits of the personal data processed, for the purpose of ascertaining whether the data is processed in accordance with the Act;
- (b) monitors the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data; and
- (c) where appropriate, makes recommendations on the need for taking legislative, administrative or other action to give protection or better protection, to the privacy of persons in respect of their personal data.

Enforcement actions by the Commissioner have not been widely publicized.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Belize?

While there are no specific ‘rules’ affecting privacy in Belize from a cultural perspective, it is expected that the fairly recent enactments of the Data Protection Act and the Cybercrime Act will significantly impact Belizean culture, as individuals and companies will be more mindful in how they treat with their own personal data and the personal data of others.

It is believed that Belizean informality in business culture may delay or dilute enforcement efforts particularly in rural areas and among small businesses.

As a multilingual and multi-ethnic society, data controllers should take care to word their privacy notices as simply and clearly as possible for the avoidance of doubt, and make them available in the languages commonly spoken in Belize.

Regulators may prioritize education and relationship-building over punitive enforcement.

Belizeans tend to resolve disputes informally, which means privacy violations may go unreported or unchallenged unless they are egregious.

The Data Protection Act includes carve-outs for small businesses, reflecting cultural and economic realities, but this can also lead to uneven enforcement across sectors.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

N/A

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Belize caters to many tourists and expats, whose information may be protected by international regulations. Therefore, international privacy laws are widely referred to by companies, and integrated into their policies, in order to reduce any liabilities that may arise from the collection of personal information.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

In 2022, the Digital Government Act was introduced, complementing the data protection framework by regulating inter-agency data sharing and digital service delivery: promoting secure and efficient use of digital technologies across government agencies and establishing oversight mechanisms for public sector data handling and privacy compliance.

Additionally, Belize's police department publicly put a proposed partnership with a facial recognition software company on hold in October 2024, citing data privacy concerns. The partnership project was intended to increase efficiency in tracking and identifying suspects but would have required sharing the country's criminal database, including criminal records and fingerprint data, with the third-party company, Biometrica.

Notwithstanding these concerns, in January 2025, the department announced its plans to install one thousand surveillance cameras equipped with similar facial recognition technology, as well as license plate reading and motion detection capabilities. The Belizean government is also reportedly working on a national ID system that will include biometric data.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Many companies lack internal privacy expertise, and formal training programs are rare. Cultural norms favor informal data sharing, which can conflict with legal requirements for consent, transparency, and data minimization.

Belizean companies often rely on foreign vendors for cloud storage, advertising, and analytics and ensuring these vendors meet adequacy standards and signing data processing agreements can be legally and logistically challenging.

Whilst the Data Protection Commissioner has enforcement powers, public enforcement actions are still rare, so companies may underestimate the risk of fines and reputational damage due to privacy violations.

12.3 What do you envision the privacy landscape will look like in five years?

With the introduction of multiple data security laws, we expect the privacy landscape to become significantly more robust. As technology continues to evolve, it's likely that these Acts will undergo future amendments to address the growing concerns surrounding online privacy.

 BOLIVIA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Bolivia.

In Bolivia, privacy is a fundamental right recognized in the State's Political Constitution. The Plurinational Constitutional Court has issued rulings that develop this right, establishing specific obligations for the protection of individual privacy.

In addition, various sectoral laws, such as Law 164 on Telecommunications and Supreme Decree 1793, require personal data protection measures in areas such as telecommunications and information technology.

The legal framework for privacy is also strengthened by Law 453 on the Rights of Users and Consumers, which protects consumers' personal information by requiring transparency and security in the processing of personal data.

1.2 What are the primary laws regulating privacy in Bolivia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The key laws in Bolivia that regulate privacy are:

- (a) Political Constitution of the State of Bolivia;
- (b) Law 164 on Telecommunications: this regulates the protection of personal data in the telecommunications and information technology sector;
- (c) Supreme Decree 1793: this regulates the processing of personal data in the ICT and telecommunications sector;
- (d) Law 453 on the Rights of Users and Consumers: this regulates the protection of personal data of consumers in all sectors, including advertising;
- (e) Penal Code: this establishes criminal penalties for privacy violations.

Furthermore, Law 453 and its regulations, Supreme Decree No 2130, are fundamental to the control of misleading advertising and the obligation to protect consumer privacy.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In Bolivia, self-regulation in the advertising sector is based on the ethical principles adopted by the industry, particularly the need for advertising to be truthful, clear, and non-deceptive. Although there is no specific regulatory framework for self-regulation, the International Chamber of Commerce ('ICC'), the Advertising and Marketing Communications Code, and other international guidelines influence advertising practices. This type of self-regulation seeks to complement existing laws, ensuring that advertising respects consumers' rights and protects their privacy. Law 453 and Supreme Decree 2130 also require truthfulness and transparency in advertising; and, in the advertising sector, agencies and advertisers adhere to these principles to avoid penalties.

1.4 How is privacy law enforced in Bolivia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy legislation in Bolivia is enforced through several mechanisms:

- (a) **Constitutional rulings:** the Plurinational Constitutional Court is key in the interpretation of rights related to privacy;

- (b) **Public regulators:** the Telecommunications and Transport Authority ('ATT') oversees practices in the telecommunications and information technology sector. The Vice Ministry of Consumer Protection, under the Ministry of Justice, enforces consumer privacy regulations, including those related to advertising;
- (c) **Self-regulation:** Industry and trade associations, such as the ICC, promote ethical principles in advertising and marketing communications.
- (d) **Private actions:** consumers can file complaints with the competent authorities if they consider that their right to privacy has been violated (eg, through misleading advertising).

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Bolivia?

In Bolivia, all companies operating within the country are subject to privacy legislation, especially those that collect, process, or store personal data. This includes both domestic and foreign companies operating in Bolivia, particularly those in the telecommunications, information technology, and financial services sectors. The legislation applies both to companies that handle personal data within Bolivia and to those whose products and services are directed at Bolivian consumers.

2.2 Does privacy law in Bolivia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

There is no specific legislation. However, privacy legislation in Bolivia applies to foreign companies under the following conditions:

- (a) Law 164 and Supreme Decree 1793 apply to foreign companies that offer services in Bolivia, operate in the country, or have Bolivian consumers; and
- (b) Foreign companies must comply with Bolivian law when their activities impact Bolivian consumers and must obtain the express consent of data subjects. If necessary, foreign companies must designate a legal representative in Bolivia to comply with local regulations.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Bolivia?

According to Supreme Decree 1793, 'personal data' is defined as any information that allows a natural or legal person to be identified. This includes data such as name, identification number, address, telephone number, email address, among others. This definition aligns with international data protection regulations.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Ruling 1738/2010-R defines 'sensitive data' as data that, by its nature, may generate discrimination or harm to the data subject. This includes information about religious beliefs, sexual orientation, biometric data, health status, among others. The regulation requires more rigorous treatment of such data, and entities that handle it must obtain the express and specific consent of the data subject, as well as ensure its confidentiality and protection.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Bolivian legislation, particularly Supreme Decree 1793, does not establish specific guidelines for the processing of anonymized, pseudonymized, or de-identified data. However, in line with international best practices, de-identified data must be handled in a way that prevents it from being easily linked to an identifiable individual. Companies must ensure that this data is not used for purposes other than its intended purpose and that its confidentiality is maintained.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies in Bolivia must comply with several key obligations under privacy law:

- (a) **Transparency:** Companies must clearly inform data subjects about the processing of their information, the purpose of the collection and the recipients of the data, according to Supreme Decree 1793;
- (b) **Consumer rights:** Companies must guarantee data subjects the rights of access, rectification, updating, cancellation, opposition and revocation of data, according to Law 453;
- (c) **Data minimization:** Only data strictly necessary to fulfill the intended purpose should be collected and processed;
- (d) **Contracts:** Companies must formalize contractual agreements with service providers or third parties that involve the processing of personal data, ensuring compliance with current regulations;
- (e) **Record keeping:** Companies must maintain adequate records of the processing of personal data to ensure traceability of the activities carried out; and
- (f) **Training:** Companies should train their staff on privacy and data protection policies, ensuring that everyone involved understands and complies with applicable regulations.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Bolivian legislation does not explicitly assign distinct roles such as ‘controller’ or ‘processor’. However, Supreme Decree 1793 establishes that companies that process personal data are responsible for compliance with data protection regulations. This implies that companies must guarantee the security, confidentiality, and appropriate use of personal data, regardless of whether they are controllers or processors.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, Bolivian law requires a legal basis for the processing of personal data. According to Supreme Decree 1793, the processing of personal data can only be carried out with the express consent of the data subject. This consent must be informed and freely given, and companies must comply with the principles of clarity, relevance, and necessity to ensure that the data is not used for purposes other than those initially disclosed.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Companies must include the following information in their privacy notices:

- (a) The identity of the person responsible for data processing;
- (b) The specific purpose for which the data is collected;
- (c) The recipients of the personal data, if applicable;
- (d) The rights of the data subject, such as access, rectification, cancellation, and objection ('ARCO rights—see question 5.2);
- (e) The legal basis for data processing; and
- (f) The ability to revoke consent at any time.

This information must be clear, accessible, and understandable, as established by Law 453 and by Supreme Decree 1793.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the following rights ('ARCO rights') in advertising contexts:

- (a) **Access:** Right to obtain information about the personal data that the company holds about them;
- (b) **Rectification:** Right to correct inaccurate or incomplete data;
- (c) **Cancellation:** Right to request the deletion of their personal data when it is no longer necessary for the purposes for which it was collected;
- (d) **Opposition:** Right to object to the processing of their data for advertising or direct marketing purposes; and
- (e) **Revocation of consent:** Right to withdraw their consent at any time, without affecting the legality of the processing carried out prior to revocation.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Businesses must obtain consumers' explicit consent before processing their personal data for marketing purposes, especially when data is collected through electronic channels (eg, emails, text messages). They must offer clear opt-out options in all marketing communications, allowing consumers to easily opt out or unsubscribe. Furthermore, they must ensure that consent is informed and freely given, and they must maintain records of the consent given.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Bolivian law requires companies that share personal data with suppliers or third parties for advertising activities to enter into clear contracts that stipulate the terms of data processing. These contracts must ensure that suppliers comply with privacy and data protection regulations, including

the obligation to guarantee information security and not use data for purposes other than those agreed upon. Supreme Decrees 1793 and 1391 require third parties to comply with the same data protection standards as the main company.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies must ensure that contracts with suppliers and third parties include clauses that:

- (a) establish that personal data will only be used for agreed purposes;
- (b) require the provider to maintain the confidentiality and security of personal data;
- (c) provide security measures and procedures for handling any data breach; and
- (d) provide auditing and monitoring mechanisms to ensure compliance with privacy regulations.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must implement due diligence measures to ensure compliance with privacy regulations, such as:

- (a) periodic audits of the processing of personal data;
- (b) ongoing staff training on data protection; and
- (c) the requirement for privacy impact assessments when conducting advertising activities that involve the use of sensitive data or the use of tracking technologies (such as cookies and pixels). These impact assessments are especially necessary when introducing new technologies or making changes to data processing processes.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

In Bolivia, direct marketing, which includes emails, text messages, and push notifications, is primarily regulated by Law 453 and Law 164. Businesses must obtain consumers' express consent before sending any direct marketing communications, ensuring that messages are clear, relevant, and non-intrusive. Additionally, they must offer an easy option for consumers to unsubscribe or opt out of future communications. Supreme Decree 1793 also requires businesses to provide adequate mechanisms for users to manage their privacy and marketing preferences.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies such as cookies, pixels, and SDKs are not specifically regulated in Bolivia. However, Law 164 and Supreme Decree 1793 require companies to obtain informed consent from users before using these technologies for data collection. Users must be informed about the purpose of data collection and the tracking methods used, and must be given the option to opt out of the use of these technologies. In practice, companies are advised to follow international best practices, such as offering a cookie banner on their websites that allows users to accept or reject the use of cookies.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions in Bolivia must comply with the general data protection principles established in Law 453. Companies must obtain consumers' express consent to collect and process their personal data within the framework of these programs, and must ensure that the data is used

only for the specific purposes of the program or promotion. Furthermore, companies must ensure that participants' personal data is treated confidentially and securely. For promotions involving raffles or prizes, specific regulations for commercial promotions must be followed, such as Law 060 on Gambling and Supreme Decrees 0781 and 0782.

7.4 How is social media and influencer marketing regulated under privacy law?

In Bolivia, social media and influencer marketing are not specifically regulated under privacy law. However, the general principles of personal data protection applicable to advertising must also be followed in these contexts. Companies that use influencers to promote products must ensure compliance with the rules of transparency and truthfulness of information, as established by Law 453. Furthermore, influencers must be informed about the processing of personal data that may be collected during marketing campaigns. Influencer marketing must be clear and not mislead about the products or services promoted.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Bolivian law does not specifically regulate targeted or behavioral advertising, but general privacy principles apply. Law 453 requires that targeted advertising complies with the principles of transparency, truthfulness, and informed consent. Companies must obtain explicit user consent before engaging in personalized advertising. Contextual advertising, which is based on the user's non-personal information, is not specifically regulated, but it must also comply with truthfulness and non-deceptive standards. The main difference between targeted and contextual advertising lies in the type of data used: targeted advertising uses the user's personal data, while contextual advertising is based on information from the user's environment or context.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution technologies and clean rooms are not specifically regulated in Bolivian legislation. However, the processing of personal data in these contexts must comply with the principles established in Law 453 and Supreme Decree 1793, which require companies to inform users about the processing of their data and obtain their express consent. Furthermore, appropriate security measures must be implemented to protect users' identity and privacy during data processing.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not specifically regulated in Bolivia. However, companies using this technology must comply with the general principles of Law 453 and Supreme Decree 1793, which require obtaining the user's informed consent before collecting location data. Furthermore, companies must ensure that data collection is limited to the minimum necessary and that location data is not used for purposes other than those previously reported.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific regulations in Bolivia governing data brokers. However, as part of their general data protection obligations, companies acting as data brokers must ensure that the data they handle is treated in accordance with the principles established in Law 453 and Supreme Decree 1793. This includes the informed consent of data subjects and the implementation of appropriate security measures to protect the information collected.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising directed at children and minors is subject to restrictions in Bolivia. Law 453 prohibits misleading or abusive advertising directed at minors and establishes that advertisements must not induce children to make decisions that could be detrimental to their well-being. Additionally, Law 259 on the Control of the Sale and Consumption of Alcoholic Beverages and Law 1280 on Tobacco prohibit the advertising of products such as alcohol and tobacco directed at minors. Advertisers must take into account the specific restrictions on the products they promote, ensuring that their advertisements do not exploit the vulnerability of minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Bolivian legislation does not specifically address profiling or the use of artificial intelligence ('AI') in the advertising context. However, the general data protection principles of Law 453 and Supreme Decree 1793 require companies to inform users about the use of these technologies, obtain their informed consent, and ensure transparency in the processing of their data. Furthermore, users must have the opportunity to object to automated decisions that significantly affect their rights, such as profiling for advertising purposes.

7.11 Are there other specific advertising practices that you wish to discuss?

In Bolivia, Andean Community Decision 486 permits comparative advertising, which must be conducted responsibly and must not mislead consumers or harm competitors. Comparative advertising must be clear and must not distort the characteristics, quality, or prices of the products being compared. Companies must ensure that comparisons are objective and based on verifiable facts.

However, note that this is just one of the advertising practices that require special attention from a privacy perspective in Bolivia. Companies must adapt their advertising strategies to comply with regulations and avoid violations that could result in sanctions.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Bolivian law establishes that international transfers of personal data must require the informed consent of the data subject. Supreme Decree 1793 stipulates that transfers outside of Bolivia are only permitted if the receiving country guarantees a level of data protection equivalent to that required by Bolivian law. Otherwise, companies must implement appropriate safeguards, such as standard contractual clauses, to ensure the data is handled securely.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Companies should be aware that data transfers must comply with the privacy and security regulations established by Law 453 and Supreme Decree 1793. There are no specific restrictions on data transfer privileges, but companies must ensure that information is transferred in a manner that does not violate the data subject's privacy rights.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Bolivia? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is regulated by Supreme Decree 1793, which establishes that companies must implement technical and organizational security measures to protect personal data. These measures must be proportional to the risk associated with data processing and must comply with the state of the art. While there are no industry-specific standards, compliance with regulations must be general and applicable to all entities that process personal data.

9.2 How are personal data breaches regulated in Bolivia? What are the requirements for notification and response?

Personal data breaches must be reported to the ATT or the Vice Ministry of Consumer Protection. The affected company must notify the relevant authority and, if those affected may suffer harm, the data subjects themselves. Notification must be made within a reasonable timeframe, preferably within 48 hours of the breach being detected.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties for non-compliance with data privacy laws in Bolivia may include fines, civil liability, and criminal liability, depending on the severity of the violation. Companies that violate data privacy regulations may be subject to administrative sanctions by competent authorities, such as the Vice Ministry of Consumer Protection or the ATT.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, consumers have the right to sue for damages caused by the improper handling of their personal data. They can seek financial compensation for the harm suffered due to the violation of their privacy. Claims can be filed in civil courts.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement agencies in Bolivia are active, and monitor both regulatory compliance and consumer complaints. The Vice Ministry of Consumer Protection and the ATT have taken steps to sanction deceptive advertising practices and the misuse of personal data in advertising campaigns. However, in terms of specific legal actions, no major public cases have been reported in recent years.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Argentina?

No specific cultural considerations have been identified that directly affect the application of privacy laws in Bolivia. However, it is important to note that data protection and privacy in the context of advertising must respect the country's social and ethical norms, such as the protection of minors and respect for human dignity.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Emerging privacy issues include the increasing use of artificial intelligence and tracking technologies in advertising. Companies should be alert to any legislative reforms that may affect how personal data is processed and protected, particularly with the increasing digitalization and globalization of markets.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

It is essential for companies to maintain a culture of compliance regarding personal data protection by implementing clear internal policies and providing ongoing privacy training to their staff. This not only ensures regulatory compliance but also improves consumer trust and minimizes the risk of penalties.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

In recent years, there has been a growing awareness of data privacy and the importance of protecting it, leading to an increased focus on regulating digital advertising and direct marketing. This has been driven by the growth of tracking technologies and the use of personal data to personalize advertising campaigns.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies face challenges related to compliance with international and local regulations, especially in a context of globalization. Growing concerns about the protection of sensitive data and emerging technologies (such as AI, and cookies) also pose complexities in data collection and management.

12.3 What do you envision the privacy landscape will look like in five years?

In five years, we’re likely to see a more regulated landscape with a greater focus on the right to be forgotten and the protection of sensitive data. Companies will need to adapt to a stricter and more sophisticated regulatory framework, which will include greater transparency in advertising practices and the use of personal data.

BOSNIA AND HERZEGOVINA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Bosnia and Herzegovina.

The legislation in Bosnia and Herzegovina ('B&H') related to privacy consists of constitutional law and statutory law.

At the state level, the right to privacy is enshrined in the Constitution of B&H. Also, the European Convention on Human Rights is directly applicable in B&H.

B&H is composed of two administrative entities—the Federation of Bosnia and Herzegovina ('FB&H') and the Republika Srpska ('RS')—along with the Brčko District ('BD'), which is a special administrative unit. Applicable rules may be adopted at the state level, in which case they apply to the entire territory of B&H; or at the entity or administrative unit level, in which case the rules apply only in the subject entity or unit (ie the FB&H or the RS or the BD).

As for statutory law, provisions related to privacy are found in various laws and by-laws regulating different areas, as noted below.

1.2 What are the primary laws regulating privacy in Bosnia and Herzegovina? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Data protection is primarily regulated at the state level of B&H by the Data Protection Act of B&H ('DPA B&H') which applies to the entire territory of B&H. A new DPA B&H has been adopted in 2025. The new DPA B&H is aligned with the European Union's General Data Protection Regulation ('GDPR') and Law Enforcement Directive ('LED').

The Communications Regulatory Agency of Bosnia and Herzegovina issues sector-specific by-laws (telecommunications and broadcasting) which contain privacy-related provisions.

There are no self-regulatory privacy frameworks in B&H.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The new DPA B&H recognizes self-regulation as an important mechanism for ensuring compliance and fostering accountability. It encourages companies to implement codes of conduct and certification mechanisms to demonstrate their commitment to data protection. However, the new DPA B&H is not yet in effect, and its implementation will begin on 5 October 2025.

The Press Council of Bosnia and Herzegovina is the only self-regulatory authority in B&H with ties to advertising and marketing practices. The Press Council of B&H is competent with regard to both print and online media. However, in practice, it has very limited authority over advertising practices in B&H.

An interested party may file an appeal against the media subject with the Press Council of B&H if the Press Code of B&H has been breached. However, the Press Council of B&H can only ask the media subject to make text corrections and denials. It cannot impose sanctions or fines.

1.4 How is privacy law enforced in Bosnia and Herzegovina? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Personal Data Protection Agency of Bosnia and Herzegovina ('PDPA') is the key regulator enforcing data protection law and its by-laws. The PDPA is in charge of the following:

- (a) supervising the application of the DPA B&H;
- (b) raising awareness of the importance of personal data protection and advising on the personal data processing;
- (c) adopting standard contractual clauses;
- (d) maintaining a list of processing related to the obligation to perform a data protection impact assessment ('DPIA');
- (e) encouraging the adoption of codes of conduct and approving such codes, as well as encouraging the establishment of data protection certification mechanisms and approving certification criteria;
- (f) approving adequate data protection measures for the transfer of data to third countries;
- (g) approving Binding Corporate Rules;
- (h) imposing fines for DPA B&H breaches and maintaining the records of DPA B&H breaches and the measures taken.

The PDPA's decisions can be challenged before the Court of Bosnia and Herzegovina.

Privacy laws are also enforced by various courts, criminal investigation authorities, and the Communications Regulatory Agency of Bosnia and Herzegovina (sector-specific).

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Bosnia and Herzegovina?

The DPA B&H applies to any company established in B&H, meaning it has a registered office or branch in B&H. The DPA B&H applies to such companies regardless of where data processing takes place.

The DPA B&H also applies to companies with no registered office or branch in B&H if they offer goods or services to individuals in B&H or monitor the behavior of individuals in B&H.

2.2 Does privacy law in Bosnia and Herzegovina apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The DPA B&H applies to foreign companies that offer goods or services to individuals in B&H or monitor the behavior of individuals in B&H.

If the company is not established in the B&H, it must designate a representative within B&H to act as a point of contact for data subjects and the PDPA. Exceptions apply if processing is occasional and does not involve large-scale processing of special categories of data.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Bosnia and Herzegovina?

Any information that allows a natural person to be identified or identifiable is considered personal data protected under the DPA B&H.

An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier, such as name, personal identification number, or to one or more factors specific to physical, physiological, psychological, economic, cultural or social characteristics of that natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

(a) **Categories of personal data considered sensitive:** The DPA B&H provides for special categories of personal data which are subject to stricter processing conditions. The special category personal data include the following:

- (i) racial or ethnic origin;
- (ii) political opinions or party affiliation;
- (iii) trade union membership;
- (iv) religious or philosophical beliefs;
- (v) health data;
- (vi) genetic data;
- (vii) data concerning an individual's sex life or sexual orientation;
- (viii) criminal records and criminal convictions; and
- (ix) biometric data.

(b) **How are they regulated differently?:** To process a special category of personal data, one of the following criteria has to be met:

- (i) The data subject has given explicit consent to the processing of personal data for specified purposes (except where a specific law provides that the data subject's consent cannot serve as the legal basis);
- (ii) Processing is necessary to carry out the obligations or to exercise rights of the controller or the data subject related to employment, social security or social protection, in so far as it is stipulated by the law or a collective bargaining agreement;
- (iii) Processing is necessary to protect the vital interests of the data subject or of another natural person (and the data subject is physically or legally incapable of giving consent);
- (iv) Processing is carried out by a foundation, association, trade union or any other non-profit organization with a political, philosophical or religious aim, in the course of its legitimate activities, with appropriate safeguards, if the processing relates solely to the members or to former members of the organization or to persons who have regular contact with the organization and the data is not disclosed outside that organization without the consent of the data subjects;
- (v) Processing relates to personal data that has been clearly and publicly disclosed by the data subject;
- (vi) Processing is carried out by a court acting in a judicial capacity or is necessary for the establishment, exercise, or defense of legal claims;

- (vii) Processing is necessary for reasons of substantial public interest, based on law that is proportionate to the aim pursued, respects the essence of data protection, and provides suitable and specific measures to safeguard the data subject's rights;
- (viii) Processing is necessary for preventive or occupational medicine, assessing an employee's working capacity, medical diagnosis, providing health or social care or managing health or social care systems, based on law or an agreement with a health professional. Such processing must be conducted or monitored by a professional bound by professional secrecy;
- (ix) Processing is necessary for the purposes related to public health, such as protecting against serious cross-border threats or ensuring high standards of health care and medicinal products, based on the law which provides for suitable measures of data protection; or
- (x) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which should be proportionate to the aim pursued, respect the substance of data protection and provide for suitable data protection measures.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The DPA B&H defines 'personal data' as any information that allows a natural person to be identified or identifiable. Thus, if the data is truly anonymized and cannot be re-identified, it falls outside the scope of the DPA B&H.

'Pseudonymization' is defined as processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organizational measures to ensure that the personal data are not attributed to a natural person. The DPA B&H recognizes pseudonymization as a security measure that can reduce risks related to personal data. Pseudonymized data remains personal data under the DPA B&H, as long as re-identification is possible.

The DPA B&H does not define de-identified data. However, if data has been de-identified but can still be linked back to a natural person, it remains personal data under the DPA B&H. On the other hand, if the data is fully anonymized, with no reasonable possibility of re-identification, the DPA B&H does not apply.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Processing has to be based on one of the six legal bases under the DPA B&H (see question 4.3).
- (b) Companies have to ensure that processing is fair and transparent, meaning data subjects must be informed about how their data is used through a clear and accessible privacy notice.
- (c) Personal data must be collected for specified, explicit and legitimate purposes and cannot be further processed in a manner incompatible with those purposes unless a valid legal basis applies.

- (d) Companies should avoid collecting excessive personal data and ensure that only the necessary amount of data is collected and processed.
- (e) Companies must ensure that personal data is accurate, complete and up-to date, by taking reasonable steps to correct or delete inaccurate or outdated data without delay.
- (f) Personal data cannot be kept for longer than necessary for the purpose for which it was collected. Companies should define data retention policies and securely delete or anonymize data when it is no longer needed. Personal data can be kept for a longer period of time if it will be processed solely for archiving purposes in the public interest or for the purpose of scientific or historical research or for statistical purposes.
- (g) Companies must take appropriate technical and organizational measures to prevent unauthorized data access, alteration, transfer or loss, as well as data misuse or destruction. Such measures include encryption, access controls, pseudonymization, and regular security assessments.
- (h) In case of a personal data breach, the company must notify the PDPA within 72 hours if there is a risk to individuals' rights and freedoms. The company should also inform the affected data subject without further delay.
- (i) A DPIA is required under the new DPA B&H when data processing is likely to result in a high risk to data subjects' rights. This includes large-scale surveillance, systematic monitoring or processing of sensitive personal data. A DPIA must assess the necessity, proportionality and risks of the processing and identify measures to mitigate those risks. If the assessment indicates a high, unmitigated risk, the controller must consult the PDPA before proceeding.
- (j) Appointing a DPO is mandatory if the company engages in large-scale systematic monitoring or processes sensitive personal data as part of its core activities. The DPO must have expert knowledge of data protection law and act independently, ensuring compliance, advising on DPIAs, and serving as the contact point for both data subjects and the PDPA. While the DPO does not bear personal liability for non-compliance, they must be involved in all data protection matters and provide the necessary resources to fulfil their role effectively. The DPO can be either the employee of a controller or a processor or act based on the services agreement.
- (j) The new DPA B&H imposes an obligation on companies to maintain internal records of processing activities. Small entities who employ fewer than 250 employees are exempt from this obligation, unless their processing is not occasional, includes special categories of data or data on criminal convictions; or poses a risk to data subjects' rights.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

The DPA B&H categorizes companies into two roles based on their processing activities: the controller and the processor:

- (a) The controller is the entity that determines the purposes and means of processing personal data.
- (b) The processor is the entity that processes personal data on behalf of the controller.

The controller has the primary responsibility for ensuring that data processing complies with DPA B&H requirements.

The controller has to enter into a data processing agreement ('DPA') with the processor. The processor must comply with the terms of the DPA and cannot subcontract or transfer the processing to another processor without the controller's prior approval.

The controller is responsible for conducting a DPIA, while the processor is required to assist the controller in conducting the DPIA and provide information to enable the controller to conduct the DPIA.

The controller is responsible for notifying the PDPA within 72 hours if a data breach occurs. The processor has to notify the controller of any data breach without undue delay.

The controller is responsible for addressing data subject rights requests (eg, access, rectification, erasure, objection, etc).

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, the DPA B&H stipulates that one of the following conditions has to be fulfilled to process personal data lawfully:

- (a) the data subject has given consent to the processing of personal data for specified purposes;
- (b) processing is necessary for the execution of a contract to which the data subject is party or for conducting actions at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for controller to comply with a legal obligation;
- (d) processing is necessary to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary to perform a task carried out in the public interest or to exercise the official authority vested in the controller;
- (f) processing is necessary to fulfil the legitimate interests of the controller or a third party, except where such interests are overridden by the interests of protecting the data subject's personal data.

As per the GDPR, the DPA B&H stipulates special requirements for minors' consent for data processing related to IT services, requiring parental/custodial approval for validity of consent given by a minor under 16.

Local legislation does not mandate a specific form of consent. However, obtaining written consent is advisable for all categories of personal data, as the DPA B&H stipulates that the controller is required to prove that the data subject has granted consent for data processing.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The DPA B&H does not impose specific requirements for privacy notices in the context of personal data processing for advertising purposes, treating them the same as privacy notices for other processing activities. The controller is required to inform the data subject of the following matters:

- (a) identity and contact details of the controller;
- (b) contact details of the DPO;
- (c) purposes of the processing for which the personal data is collected;

- (d) legal basis for the processing;
- (e) legitimate interests pursued by the controller or a third party (if processing is based on legitimate interests);
- (f) recipients or categories of recipients of the personal data, if any;
- (g) intention to transfer personal data to a third country or international organization, and if so, details of the appropriate safeguards;
- (i) data retention period;
- (j) data subject rights;
- (k) right to withdraw consent at any time;
- (l) right to lodge a complaint with the PDPA;
- (m) whether providing data is a statutory or contractual requirement, and the consequences of failing to provide the data; and
- (n) existence of automated decision-making, including profiling.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) Consumers have the right to be informed about how their personal data is collected, used, and shared for advertising purposes. Please see question 5.1 for a more detailed list of information that should be provided to consumers.
- (b) If advertising relies on consent as a legal basis, consumers have to be able to withdraw their consent at any time. In case of a direct marketing, consumers have the right to object to the processing of their personal data at any time. Once an objection is made, the company must stop processing the data.
- (c) If the processing of personal data is based on the controller's legitimate interest, the consumer has the right to object to the processing on grounds relating to the specific situation. The controller must cease processing the personal data unless it can demonstrate compelling legitimate grounds for the processing that override the consumer's rights or for the defense of legal claims.
- (d) Consumers can request access to their personal data to understand what information is being processed, how it is being used, and with whom it has been shared. If personal data used in advertising is inaccurate or incomplete, data subjects have the right to request corrections. Consumers can also request the deletion of their personal data, particularly if it is no longer necessary for the purpose it was collected or if they withdraw consent. Consumers can request that their data be restricted from processing, meaning it can only be stored and not used for advertising.
- (e) If advertising processing is based on consent or contract and is carried out by automated means, consumers have the right to receive their personal data in a structured, commonly used, and machine-readable format and the right to have it transmitted to another controller.
- (f) Consumers have the right not to be subject to decisions based solely on automated processing, including profiling, if such decisions significantly affect them.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Consent is required when personal data is processed for advertising purposes and no other legal basis applies. The data subject must have the right to withdraw consent at any time.

For direct marketing, companies must provide an opt-out mechanism. If the data subject objects to processing for direct marketing purposes, the personal data cannot be processed for such purposes.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The DPA B&H stipulates that if a company engages vendors to process personal data on its behalf, a DPA has to be concluded between the parties. The vendor cannot subcontract or transfer the processing to another entity without the controller's prior approval. The DPA should:

- (a) define the processing scope, purposes and duration;
- (b) obligate the processor to follow the controller's instructions;
- (c) require confidentiality among employees processing the data;
- (d) ensure appropriate security measures;
- (e) prohibit sub-processing without the controller approval;
- (f) mandate assistance with data subject rights and compliance obligations.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When disclosing or receiving personal data from vendors or third parties, companies must:

- (a) conclude a DPA for processors;
- (b) conclude a joint controller agreement if two companies jointly determine the purpose and means of processing;
- (c) ensure a lawful basis for data sharing and compliance with the DPA B&H and controller's bylaws regulating data protection for independent controllers; and
- (d) comply with rules regulating international transfer of personal data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

A DPIA is required under the new DPA B&H when data processing is likely to result in a high risk to data subjects' rights. This includes large-scale surveillance, systematic monitoring or processing of sensitive personal data. A DPIA must assess the necessity, proportionality and risks of the processing and identify measures to mitigate those risks. If the assessment indicates a high, unmitigated risk, the controller must consult the PDPA before proceeding.

Both the controller and the processor must take appropriate technical and organizational measures to prevent unauthorized data access, alteration, transfer or loss, as well as data misuse or destruction. Such measures include encryption, access controls, pseudonymization, and regular security assessments.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The DPA B&H specifies a general opt-out regime for direct marketing, meaning that data subjects have the right to object at any time to the processing or transfer of their personal data for marketing purposes. Additionally, individuals must be notified before their personal data is shared with a third party for marketing.

Marketing communications must be clear and unambiguous to ensure transparency.

The Communications Regulatory Agency may maintain an opt-out register for email marketing, though this is not explicitly addressed in the new DPA B&H.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies (cookies, pixels, SDKs) is regulated under the general rules of personal data protection, particularly regarding consent and the obligation to inform users about the collection and use of their data.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs that involve data collection must comply with the principles of purpose limitation and data minimization. Individuals must be informed about data use and have the right to withdraw consent.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media is not explicitly regulated by the B&H legal system; therefore the general rules on personal data protection apply.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Behavioral and targeted advertising are not explicitly regulated under the DPA B&H. However, they fall under general data protection rules, particularly that which allows users to object to their personal data being used for marketing purposes. Advertisers must obtain valid user consent for such processing.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

While digital identity resolution and clean room technologies are not explicitly regulated, they must comply with the general data protection framework under the DPA B&H. This includes lawful data processing, user transparency, consent mechanisms, security safeguards, and data minimization principles to ensure privacy protection.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising falls under the general rules of the DPA B&H. Advertisers must obtain explicit user consent, ensure transparent data processing, allow users to withdraw consent, and implement security measures to protect location data.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are not explicitly defined or regulated; hence they are subject to general data protection obligations as data controllers or processors. This includes lawful data collection, transparency, user rights, security measures, and restrictions on data transfers.

7.9 How is advertising to children and minors regulated under privacy law?

The DPA B&H does not explicitly regulate advertising to children; however, advertisers must obtain parental consent, ensure transparency, and avoid behavioral tracking unless legally justified. Additionally, sensitive data processing is strictly regulated, and violations can lead to severe penalties.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The DPA B&H imposes strict regulations on the use of personal data for advertising purposes. It emphasizes the necessity of obtaining consent for data processing activities, especially when involving profiling and automated decision-making, and mandates robust safeguards to protect individuals' privacy rights. The new DPA B&H specifically addresses the use of automated decision-making, including profiling, and prohibits such practices if they significantly affect the individual, unless:

- (a) the data subject has given explicit consent;
- (b) the processing is necessary for the performance of a contract or for compliance with legal obligations; or
- (c) it is based on the legitimate interests of the data controller, provided these interests are not overridden by the rights and freedoms of the data subject.

7.11 Are there other specific advertising practices that you wish to discuss?

To the best of our knowledge, there are no specific advertising practices in B&H that should be emphasized or discussed at this time.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Personal data can be transferred outside B&H only if the receiving country provides adequate security measures. If the recipient country does not have adequate protections, transfers may still occur under specific conditions such as explicit user consent, contractual safeguards, or legally required exemptions.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The new DPA B&H establishes a framework for international data transfers that aligns with European standards, emphasizing the importance of data subject consent, contractual necessity, public interest, and adequate safeguards. While it doesn't specifically address legal privileges, the overarching principle is clear: personal data transfers must be conducted with a high degree of care, ensuring that individuals' rights and freedoms are not compromised.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Bosnia and Herzegovina? Are there minimum standards? Does this differ by sector or size of the entity?

B&H's current data security regulations provide a general framework applicable to all entities processing personal data, emphasizing the implementation of appropriate security measures without distinguishing based on sector or entity size.

As the legal landscape evolves, particularly with efforts to align more closely with EU standards, it is advisable for organizations to stay informed about potential legislative updates that may introduce sector-specific or size-based requirements.

9.2 How are personal data breaches regulated in Bosnia and Herzegovina? What are the requirements for notification and response?

Data controllers must notify the PDPA within 72 hours if a breach is likely to risk individuals' rights.

If the breach poses high risks, affected individuals must also be informed.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The DPA B&H stipulates that fines for violations can range from BAM 20,000 to BAM 40 million (approx €10,000–€20 million), or up to 4% of a company's total global annual turnover from the previous financial year, whichever is higher. The DPA B&H empowers the PDPA to enforce compliance, ensuring that organizations adhere to established data protection principles. Organizations operating within B&H should take proactive steps to ensure full compliance with these regulations to avoid substantial fines and reputational harm.

10.2 Do consumers have a private right of action? What remedies are available to them?

The new DPA B&H provides that data subjects have a private right of action against data controllers or processors. The DPA B&H explicitly grants individuals the right to seek judicial protection if they believe their rights under the law have been violated due to the processing of their personal data. This means that consumers can directly sue entities responsible for unlawful data processing, without necessarily relying on administrative complaints to the PDPA.

Additionally, the new DPA B&H guarantees the right to compensation for material and non-material damages suffered because of a data protection violation. It also establishes joint liability for controllers and processors, meaning that multiple entities involved in unlawful processing may be held responsible.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The PDPA plays an active role in monitoring compliance and has, in practice, issued fines and corrective orders where it has identified breaches under the applicable law. The PDPA is actively engaged in enforcing data protection laws in B&H, with the authority to address violations across

various sectors, including advertising. While specific enforcement actions related to advertising have not been prominently documented, the PDPA's broad enforcement capabilities ensure that advertising practices comply with established data protection standards.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Bosnia and Herzegovina?

Privacy awareness is growing in B&H, leading to increased regulatory scrutiny and public expectations for compliance.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Key issues include:

- (a) AI-driven profiling risks;
- (b) cross-border compliance complexities; and
- (c) user consent management.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Businesses should adopt a proactive compliance strategy, including:

- (a) regular audits;
- (b) employee training; and
- (c) transparent privacy policies.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The new DPA B&H aligns B&H with GDPR, strengthening user rights and corporate obligations. The new legal reform introduces a set of provisions strengthening data subject rights, enforcement mechanisms, and alignment with EU GDPR standards. Unlike the 2022 law, which primarily allowed data subjects to file complaints with the PDPA, the 2025 law explicitly grants them the right to file lawsuits against controllers and processors and claim compensation for material and non-material damage. Enforcement has also been enhanced, with higher fines and corrective orders allowing the PDPA to halt unlawful processing activities more effectively. These changes were triggered by B&H's EU integration efforts, increasing data security risks, and public demand for stronger privacy rights, marking a significant shift towards greater corporate accountability and individual data protection.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies must navigate increasingly complex and stringent consent mechanisms under evolving privacy laws. With the tightening of requirements for explicit, informed, and granular consent, organizations face significant challenges in ensuring compliance while maintaining transparency and respect for data subject rights. Failure to adequately manage these requirements can lead to substantial legal and financial repercussions, including fines and reputational damage.

12.3 What do you envision the privacy landscape will look like in five years?

The growing scrutiny of cross-border data transfers presents a critical challenge for multinational organizations. Data transfer restrictions, particularly in jurisdictions that do not offer equivalent levels of data protection require businesses to implement sophisticated compliance frameworks, such as Standard Contractual Clauses ('SCC's) and Binding Corporate Rules ('BCR's), to avoid breaches of international privacy regulations.

 BRAZIL 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Brazil.

The Federal Constitution ('CF') establishes fundamental principles that safeguard privacy, personal data, and the confidentiality of information. In this regard, the CF provides for the inviolable right to intimacy, privacy, honor, and image; and the confidentiality of correspondence, telegraphic communications, data, and telephone communications. A violation of these rights entitles the affected individual to compensation for moral or material damages. In 2022, this list of fundamental rights was expanded to include personal data protection. The amendment also granted the Federal Government exclusive authority to legislate on the matter.

As for the Brazilian Civil Code, although it does not explicitly define 'privacy', it establishes that an individual's private life must not be violated. It further empowers judges, upon request, to take necessary measures to prevent or halt any act that infringes this right. Additionally, it affirms that the right to privacy is personal, non-waivable, and non-transferable.

The first and principal specific legislation on data protection in Brazil, the General Data Protection Law (Federal Law 13,709/2018) ('LGPD'), was enacted in August 2018 and took effect in September 2020. The LGPD aligns with the global movement toward stronger protection for personal data, granting extensive rights to data subjects and imposing significant obligations on data processing agents. Whilst inspired by the European GDPR, the LGPD also introduces new regulatory provisions tailored to the Brazilian legal framework.

1.2 What are the primary laws regulating privacy in Brazil? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The LGPD is the primary law regulating privacy matters in Brazil. It established the National Data Protection Authority ('ANPD'), responsible for overseeing, implementing, and enforcing compliance with the LGPD (see further question 1.4).

From an advertising standpoint, the Brazilian Advertising Self-Regulation Code ('CONAR Code') serves as the primary framework, though non-binding, for advertising practices in Brazil (see question 1.3).

However, other legal frameworks also indirectly govern the processing of personal data for advertising purposes. These laws cover more general aspects, including publicity rights, transparency, and consumer protection.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

One of the key self-regulatory frameworks is the Brazilian Advertising Self-Regulation Code, enforced by the National Advertising Self-Regulation Council ('CONAR'). The CONAR Code establishes ethical standards for advertising, including rules on transparency, consumer protection, and the responsible use of personal data in marketing campaigns.

Another relevant self-regulatory initiative is the Self-Regulatory Code for the Practice of Email Marketing ('CAPEM'), which governs email marketing practices (see question 7.1).

While these self-regulatory mechanisms are not legally binding, they are widely respected within the advertising industry. Additionally, Brazilian courts and regulatory authorities often consider compliance with self-regulatory standards when assessing cases related to advertising and data privacy.

1.4 How is privacy law enforced in Brazil? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The ANPD is the administrative body responsible for overseeing personal data protection and is empowered to regulate, monitor, guide, prevent, and impose sanctions. Since its creation, the ANPD has actively worked to foster discussion and disseminate privacy and data protection concepts, practices, and principles, publishing various materials to raise awareness and regulate the LGPD.

The ANPD's monitoring activities involve collecting information and data to support decision-making and ensure the proper functioning of the regulated environment. Its guidance efforts focus on promoting awareness and education among data controllers and data subjects. Prevention entails collaborating with regulated entities to address or avoid issues that may impact data subjects and other stakeholders. Repression, on the other hand, is a more coercive approach aimed at halting harmful practices, ensuring compliance, and applying sanctions through administrative sanctioning processes, which may or may not be preceded by preparatory procedures.

In 2021, the ANPD Board of Directors approved the Regulation on Oversight and Administrative Sanctioning Processes, which sets forth the procedures for the oversight process, including monitoring, guidance, and preventive actions, as well as the rules governing the ANPD's administrative sanctioning process. In 2023, the administrative sanctioning process was further clarified, ensuring greater legal certainty and transparency for the parties involved. However, whilst, in 2023, the ANPD released a list of administrative sanctioning proceedings, this list is out-of-date, as the ANPD has been stepping up its enforcement activities by applying corrective measures for non-compliance with the law, resulting in a significant increase in the number of sanctioning proceedings since its publication.

In addition to the ANPD, the protection of personal data in Brazil also involves the judiciary and consumer protection agencies, such as Procon. The judiciary plays a fundamental role in safeguarding the rights of data subjects through decisions that interpret and apply the LGPD in specific cases. Brazilian courts have consolidated jurisprudence on privacy and data protection issues, ensuring the effectiveness of the rights provided in the law. Procon, on the other hand, can intervene in cases where companies violate data protection rules and ensuring that consumer rights are respected, thus complementing the protection of personal data in Brazil.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Brazil?

The LGPD applies to any company that collects personal data from individuals located in Brazil, processes data in Brazil, or offers goods and services to individuals in Brazil. However, the LGPD does not apply to:

- (a) activities conducted exclusively for the purposes of public security, national defense, state security, or the investigation and prosecution of criminal offenses;
- (b) data that originates from or is destined for other countries, provided it is merely transiting through Brazil;

- (c) personal or non-commercial use; or
- (d) journalistic, artistic, or academic purposes.

2.2 Does privacy law in Brazil apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. The LGPD establishes the principle of extraterritoriality in its application. As a result, its provisions apply not only to companies based in Brazil, but also to foreign entities that process or collect data within Brazilian territory, as well as to foreign companies that seek to offer or provide goods and services to individuals located in Brazil.

Regarding the necessity of a local representative, it is worth noting that appointing a data protection officer ('DPO') is mandatory for all data-controlling companies that process personal data, except for small-scale processing agents. In this sense, one of the key requirements for the DPO is the ability to communicate clearly and accurately in Portuguese; however, the DPO does not necessarily need to be located in Brazil.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Brazil?

According to the LGPD, 'personal data' refers to any information related to an individual who can be directly identified by that information, or who can potentially be identified from it.

For each type of data, the LGPD establishes different guidelines to be followed during processing activities, with specific limitations on the conditions and legal bases under which personal and sensitive data may be processed.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

'Sensitive data' includes any personal data related to racial or ethnic origin, religious belief, political opinion, trade union membership, or affiliation with a religious, philosophical, or political organization, as well as data concerning health, sexual life, genetic, or biometric information when linked to an individual.

Given the potential for discrimination, processing sensitive personal data is only allowed under specific legal bases (see question 4.3).

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under the LGPD, the treatment of anonymized, pseudonymized, or de-identified data is as follows:

- (a) **Anonymized data** is not considered personal data under the LGPD, as it has been processed in such a way that the data subject can no longer be identified, and the anonymization process cannot be reversed. Since anonymized data does not identify individuals, it is not subject to the provisions of the LGPD, meaning it is not regulated by the law, and there are no obligations or restrictions regarding its processing.

- (b) **Pseudonymized data**, on the other hand, still contains elements that can identify a data subject, though these elements are encrypted or masked. The pseudonymization process is reversible, meaning that the data subject could potentially be re-identified. Therefore, pseudonymized data is treated as personal data under the LGPD and is subject to its principles, rules, and requirements.
- (c) **De-identified data** refers to data that has been processed to remove identifying information. However, the key difference between de-identified and anonymized data is that de-identification can still be reversed, and re-identification could potentially occur under certain circumstances. If re-identification is possible, de-identified data may still fall under the LGPD's definition of personal data and is subject to the law's provisions.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

There are ten principles that can be considered the key obligations that companies must adhere to when processing personal data under the LGPD:

- (a) **Purpose**: Processing must be for legitimate, specific, explicit, and informed purposes, and further processing must not be incompatible with these purposes;
- (b) **Adequacy**: Processing must be compatible with the purposes informed to the data subject;
- (c) **Necessity**: Processing must be limited to the minimum required to achieve its purposes, ensuring that the data collected is relevant, proportionate, and not excessive in relation to the purpose of processing;
- (d) **Free access**: Data subjects must be guaranteed easy and free access to information regarding the form, duration, and completeness of the processing of their personal data;
- (e) **Quality of data**: Personal data must be accurate, clear, and up-to-date;
- (f) **Transparency**: Data subjects must be provided with clear and accurate information about the processing of their personal data;
- (g) **Security**: Effective technical and administrative measures must be implemented to protect personal data;
- (h) **Prevention**: Measures must be adopted to prevent harm caused by the processing of personal data;
- (i) **Non-discrimination**: Personal data should not be used for discriminatory purposes; and
- (j) **Liability and accountability**: Data processing agents must demonstrate the adoption of effective measures to prove compliance with personal data protection rules, ensuring the effectiveness of these measures.

Moreover, the following obligations must be observed:

- (k) Processing agents (ie, data processors and controllers) should inform the data subject, in a clear and specific manner, of any changes in the purpose, form, or duration of data processing, as well as changes regarding the sharing of the personal data or identification of the controller.
- (l) The processor must process the data according to the instructions provided by the controller.
- (m) The controller and the processor must keep a record of the personal data processing operations that they perform, especially when based on legitimate interest.

- (n) The ANPD may require the controller to draw up a report on the impact of its data processing operations on the protection of personal data, including sensitive data, under the terms of the LGPD. Such report must contain at least:
 - (i) a description of the types of data collected;
 - (ii) the methodology used for the collection and for ensuring the security of the information; and
 - (iii) the controller's analysis regarding the measures, safeguards, and risk mitigation mechanisms adopted.
- (o) The controller must appoint a DPO for the processing of personal data. The identity and contact information of the DPO must be disclosed publicly, clearly, and objectively, preferably on the controller's website.
 In May 2022, the ANPD issued 'Guidelines for Definitions of the Personal Data Processing Agents and DPOs' which provides guidelines regarding the role and its attributions. The activities of the DPO consist of:
 - (i) receiving complaints and communications from data subjects, providing clarification and adopting measures to solve issues;
 - (ii) receiving communications from the ANPD;
 - (iii) advising the entity's employees and contractors regarding the practices to be taken in relation to the protection of personal data; and
 - (iv) performing other duties as determined by the controller or as set out in complementary rules.
- (p) Except in specific situations, the processing agent must delete personal data upon the completion of the data processing, which may occur when the purpose of the data processing is reached, when the period agreed for the processing ends, when requested by the data subject, or when ordered by the competent body. The specific situations in which the processing agent will not delete the personal data after the end of its processing are where the personal data are required for:
 - (i) compliance with legal or regulatory obligation by the controller;
 - (ii) study by a research body, ensuring, whenever possible, anonymization of personal data;
 - (iii) transfer to a third party, provided that the data processing requirements laid down in the LGPD are respected; or
 - (iv) exclusive use of the controller, as long as the data is anonymized and third-party access is forbidden.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. In addition to the data subject, there are three other figures involved in data processing:

- (a) **Processor**—a natural or legal person, under public or private law, who processes personal data on behalf of the controller;
- (b) **Controller**—a natural or legal person, whether public or private, who takes the decisions concerning the processing of personal data; and
- (c) **Data Protection Officer ('DPO')**—a natural or legal person, appointed by the controller, who acts as a communication channel between the controller, the data subject and the competent authority.

Each role affects their obligation. The ANPD's 'Guidelines for Definitions of the Personal Data Processing Agents and DPOs' provide guidelines regarding each role and its attributions. For example, any controller or processor who, in connection with the performance of the activity of personal data processing, causes any property, moral, individual, or collective damage to any third parties, in violation of the LGPD, is required to indemnify them.

Additionally, in order to ensure effective compensation to the data subject, the LGPD provides joint liability between the controller and the processor in cases when:

- the damage was caused by a processing activity carried out by the processor after breaching the data protection law obligations provided in the LGPD; or
- the processor has not followed the controller's lawful instructions.

However, processing agents (ie, controllers and processors) will not be held responsible where they can prove that:

- they have not processed personal data;
- although they have processed personal data, there has been no violation of the LGPD; or
- the damage is due to the sole fault of the data subject or a third party.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

(a) The LGPD establishes the following legal bases that authorize the processing of personal data (except for data classified as sensitive):

- (i) Data subject's consent;
- (ii) Fulfilment of a legal or regulatory obligation;
- (iii) By the public administration, for implementing public policies established by law;
- (iv) For conducting studies by research bodies, provided that anonymity is maintained;
- (v) Whenever necessary for the performance of contracts or preliminary steps relating to agreements to which the data subject is a party, at the request of the data subject;
- (vi) For the regular exercise of rights in judicial, administrative, or arbitral proceedings;
- (vii) For protecting the life or physical integrity of the data subject or a third party;
- (viii) For health protection, with procedures carried out by health professionals or entities;
- (ix) For the protection of credit, in accordance with the Brazilian Consumer Defense Code;
- (x) When necessary to meet the legitimate interests pursued by the controller or a third party (unless such interests are overridden by the data subject's rights and freedoms, requiring data protection).

(b) The legal bases for processing sensitive personal data (see question 3.2) are:

- (i) Explicit consent by the data subject or their legal representative to such processing for specific purposes; or
- (ii) In any event, when processing is essential:
 - for compliance with a legal or regulatory obligation by the controller;
 - for enforcement by public authorities of public policies set by law or regulation;
 - for conducting studies by research bodies, ensuring anonymization of sensitive data whenever possible;
 - for the regular exercise of rights, including in contracts and lawsuits, administrative or arbitration proceedings;

- for protecting the life or physical safety of the data subject or a third party;
- for health protection in procedures carried out by health professionals or health entities; or
- to prevent fraud and ensure security in processes of identification and authentication in electronic systems, safeguarding the fundamental rights and freedoms of data subjects.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the LGPD, companies processing personal data for advertising purposes must clearly state the purpose of processing, the legal basis, and the rights of data subjects, including opting out of targeted ads (see question 7.1). They must also specify the categories of collected data, any sharing with third parties or international transfers, the data retention period, security measures in place, and provide the DPO contact details for privacy-related inquiries.

Additionally, when the processing of personal data is based on consent, it is essential that such consent be a free, informed, and unambiguous expression by which the data subject agrees to the processing of their personal data for this specific purpose.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers, who are also data subjects, have the right to obtain from the controller, at any time and upon request, with respect to the data processed:

- (a) confirmation of the existence of processing;
- (b) access to the personal data;
- (c) correction of incomplete, inaccurate, or outdated data;
- (d) anonymization, blocking, or deletion of unnecessary, excessive, or unlawfully processed data;
- (e) portability of the data to another service or product provider;
- (f) deletion of personal data processed with the data subject's consent;
- (g) information on public and private entities with which the controller has shared data;
- (h) information on the possibility of withholding consent and the consequences of refusal;
- (i) withdrawal of consent; and
- (j) file a petition with the ANPD.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Typically, advertising activities rely on either consent or legitimate interest as their legal basis. While legitimate interest requires the company to demonstrate that data processing does not infringe on data subjects' rights, consent must be specific, explicit, and informed.

For advertising activities, legitimate interest can be applied through the soft opt-in approach, provided that three key conditions are met:

- (a) there is a pre-existing relationship between the data controller and the data subject;
- (b) marketing efforts are strictly limited to offering products or services similar to those previously sought or contracted; and
- (c) a clear and easily accessible opt-out mechanism is available both at the time of data collection and in all future communications.

Regardless of the chosen legal basis—consent or legitimate interest—all advertising-related processing must include an opt-out mechanism, ensuring that data subjects can easily unsubscribe from the company’s database.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Under the LGPD, the use of vendors and third parties in advertising—such as agencies, DSPs, SSPs, and data providers—must be based on a valid legal basis and uphold transparency by informing data subjects about data sharing and its intended purposes. In practice, it is essential to provide mechanisms that allow data subjects to track how their data is processed and shared, as well as with whom. At a minimum, companies must disclose the specific profile of the entities receiving the data, including their sector, industry, and the type of services or products they offer, along with their name.

Companies must also implement contractual safeguards with vendors, enforce robust security measures, and ensure full compliance with data protection obligations. If data is transferred internationally, it must align with the LGPD’s cross-border data transfer requirements (see question 8.1). Additionally, data subjects must be provided with clear and easily accessible opt-out options.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When disclosing or receiving personal data from vendors or third parties, companies must establish contractual obligations to ensure compliance with data protection requirements. Key obligations include but are not limited to:

- (a) Clearly specify whether the parties act as controllers, processors, or joint controllers and outline their respective responsibilities;
- (b) Ensure that data processing is justified by a valid legal basis and only for specified and legitimate purposes;
- (c) Require vendors to implement technical and organizational security measures to protect personal data against unauthorized access, loss, or misuse;
- (d) Impose obligations on vendors to maintain confidentiality, comply with LGPD principles, and adhere to best practices in data protection;
- (e) Ensure that vendors cooperate in enabling data subjects to exercise their rights, including access, correction, deletion, portability, and consent withdrawal;
- (f) Prohibit vendors from using the data for unauthorized purposes or sharing it with other parties without the controller’s approval;
- (g) Require vendors to immediately notify the controller in case of a security incident and assist in investigating and mitigating risks;

- (h) If data is transferred outside Brazil, contracts must ensure compliance with LGPD's cross-border transfer requirements, such as standard contractual clauses or adequacy decisions;
- (i) Grant the company the right to audit the vendor's compliance with contractual obligations and applicable data protection laws; and
- (j) Establish conditions for contract termination, including requirements for returning or deleting personal data upon contract expiration or at the controller's request.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

There are numerous practices that must be observed when processing personal data, such as adopting security, technical, and administrative measures to protect personal data from unauthorized access and accidental or unlawful incidents of destruction, loss, alteration, disclosure, or any form of improper or unlawful processing.

The controller is required to notify the ANPD and the data subject in the event of a security incident that may pose a risk or significant harm to data subjects. Furthermore, processing agents, within their respective roles, may establish best practices and governance rules that define organizational conditions, operational frameworks, procedures—including data subjects' complaints and requests—security standards, technical requirements, specific obligations for those involved in processing, educational initiatives, internal supervision and risk mitigation mechanisms, and other aspects related to personal data processing.

Under the LGPD, a data protection impact assessment ('DPIA') is a document prepared by the controller that outlines personal data processing activities that may pose risks to civil liberties and fundamental rights, along with the measures, safeguards, and risk mitigation mechanisms in place. It is worth noting that the ANPD may request the controller to provide a DPIA when processing is based on legitimate interest, while respecting trade and industrial secrets.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Brazil generally follows an opt-in system, meaning that a data subject's consent must always be explicit and can never be implied. More specifically, before a company sends marketing communications—such as emails, text messages, or push notifications—the data subject must provide express consent for this purpose. Without such consent, unsolicited advertisements must not be sent.

Since 2009, email marketing has been regulated by CAPEM. CAPEM introduces an exception to the opt-in rule when:

- (a) there is a pre-existing relationship between the data controller and the data subject;
- (b) marketing efforts are strictly limited to offering products or services similar to those previously sought or contracted; and
- (c) a clear and easily accessible opt-out mechanism is available both at the time of data collection and in all future communications.

In such cases, companies may send marketing emails under a soft opt-in system, meaning explicit consent is not required.

All marketing communications must include an opt-out mechanism, allowing data subjects to unsubscribe from the company's database. Additionally, data subjects must be informed of the deadline for the removal of their contact information. The LGPD also mandates that personal data obtained through consent may only be shared with the data subject's specific authorization.

Notably, the Brazilian Superior Court of Justice has ruled that marketing calls made to consumers at home or work using coercive or deceptive tactics and without prior approval constitute 'abusive publicity' and are therefore illegal under the Brazilian Consumer Defense Code.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

In October 2022, the ANPD published the 'Guidance on Cookies and Personal Data Protection', outlining key interpretations regarding the use of cookies and other online tracking technologies. In relation to the LGPD, the following provisions stand out:

- (a) The collection of personal data through cookies must be limited to the minimum necessary to achieve legitimate, explicit, and specific purposes, ensuring that further processing is not conducted in a manner incompatible with those purposes. In this sense, the purpose justifying the use of a specific category of cookies must be clearly defined and communicated to the data subject, and the data collection must align with that purpose;
- (b) There is an obligation of the data agents to provide data subjects with clear, precise, and easily accessible information regarding the processing of their data, the retention period, and the specific purposes justifying data collection through cookies. Additionally, it is essential to inform them about any potential data sharing with third parties and the rights granted to data subjects;
- (c) The retention period of cookies must align with the purposes of processing, being limited to what is strictly necessary to achieve those purposes. Therefore, indefinite, excessive, or disproportionate retention periods concerning the intended purposes are not compliant with the LGPD; and
- (d) Whenever the use of cookies involves the processing of personal data, it will only be permitted if the data controller identifies a valid legal basis and complies with the specific requirements established by the LGPD.

7.3 How are loyalty programs and promotions regulated under privacy law?

Besides the LGPD, loyalty programs and promotions are also subject to the following regulations:

- (a) **Consumer Defense Code** (Federal Law 8,078/90): This law establishes the legal framework for consumer relations in Brazil, covering product and service liability, contractual clauses, commercial practices, advertising, and the provision of relevant information to consumers. It strictly prohibits misleading and abusive advertising. Additionally, consumers have the right to access their personal data and its sources in consumer databases and records. Any consumer reference file that is not created at the consumer's request must be formally communicated in writing.
- (b) **CONAR Code**: Any activity aimed at stimulating the consumption of products and services or promoting institutions, concepts, or ideas is considered advertising and must comply with the CONAR Code. Although not a formal law, Brazilian courts have consistently upheld the rulings of the CONAR Council when challenged. As a result, the CONAR Code is widely recognized as a reference document and is often treated as subsidiary legislation.

- (c) **Decree-Law 70,951/72 and Ordinance 7,638/2022:** These laws require prior authorization from a regulatory body linked to the Ministry of Finance for any promotion involving the free distribution of prizes, such as contests, sweepstakes, and gift certificates.
- (d) **Electronic Commerce Decree** (Decree-Law 7,962/2013): This law governs consumer relations in online transactions and establishes specific requirements for e-commerce activities.

7.4 **How is social media and influencer marketing regulated under privacy law?**

The privacy provisions established in the LGPD and other laws referred to in question 1.2 must be observed.

Based on these laws, even though not explicitly mentioned, several precautions must be taken when processing personal data derived from social media and influencer marketing. For example, photographs and videos related to a person's profile may be considered biometric data depending on the context and, therefore, classified as sensitive data under the LGPD (see question 3.2). Consequently, legitimate interest does not qualify as a valid legal basis in this scenario.

Except in specific cases, the use of images or videos featuring individuals or groups of individuals who are identified or identifiable for marketing purposes must be based on the legal ground of consent. Conversely, if the content of a photo or video used on social media does not allow for the identification of individuals or small groups but is purely generic (eg, an image of crowds or public places without identifiable individuals), it does not contain personal data and is not subject to LGPD regulations.

In 2021, the CONAR released the 'Digital Influencer Advertising Guidelines', which provide guidance on applying the CONAR Code to commercial content on social media, particularly content created by digital influencers.

7.5 **How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

There are no specific privacy regulations governing targeted or behavioral advertising. However, the privacy provisions established in the LGPD and other laws must be observed. In general, the data subject's consent is required for targeted and behavioral advertising.

The ANPD is expected to issue regulations addressing currently unregulated aspects.

7.6 **How are digital identity resolution and clean room technologies regulated under privacy law?**

Under the LGPD, both digital identity resolution and clean room technologies must comply with principles stated in the law, such as transparency, security, and purpose limitation (see question 4.1).

Identity resolution requires a valid legal basis, such as consent or legitimate interest, and data subjects must be informed about data collection, processing, and sharing. Individuals also have rights to access, correct, delete, and object to data processing.

Clean rooms, while designed to enhance privacy, remain subject to LGPD if they involve identifiable data. Anonymized data falls outside the law's scope.

7.7 How is location-based advertising regulated under privacy law?

The LGPD does not specifically mention location-based advertising; however, the processing of geolocation data for targeted advertising purposes must comply with its general provisions on personal data protection. This includes, for example, ensuring a valid legal basis, providing clear and transparent privacy notices, respecting data subject rights, and adopting security measures to protect geolocation data.

The ANPD is expected to issue regulations addressing currently unregulated aspects.

7.8 How are data brokers defined and regulated under privacy law?

Although the LGPD does not explicitly address data brokers, indirect marketing takes place when businesses use data obtained from these brokers to create detailed consumer profiles and target specific advertising campaigns to these groups based on behaviors, interests, or demographic traits. This practice is legitimate, provided it adheres to basic principles of the LGPD, such as control, transparency, and quality. When consent is the legal basis for data processing, it is essential to respect the scope of that consent: consent for data sharing between company A and company B applies only to that specific transaction and should not extend to further sharing, such as from B to company C. The consent should always be understood in its specific context and not interpreted broadly.

7.9 How is advertising to children and minors regulated under privacy law?

Processing of children's (under 12 years old) data can only occur after obtaining a specific consent given by at least one parent or legal guardian of the child. A child's personal data may be collected without this consent when collection is necessary:

- (a) to contact the parent or legal guardian if used a single time and without storage, or
- (b) for the protection of the child.

Also, controllers may not subject the participation of children in games, internet applications, or other activities to a requirement to provide personal data beyond what is strictly necessary for the activity.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Under the LGPD, profiling and the use of AI or automated decision-making for advertising must comply with principles stated in the law (see question 4.1). Companies must inform individuals about the existence of automated processing, including profiling, and provide clear information on the criteria and consequences of such decisions.

Profiling involves the processing of personal data, either automated or not, to assess specific patterns related to an individual. This practice can be applied broadly or to specific areas, such as analyzing consumption habits, health conditions, financial status, or productivity. In cases where personal data is processed automatically for profiling purposes, it is crucial to note that the more intrusive the practice—especially when it involves deeply personal or potentially sensitive information—the higher the risk of harm to individuals and the greater the likelihood of violating the LGPD. Consequently, it may be necessary to evaluate requests from data subjects to review decisions made solely by systems relying on artificial intelligence or other automated processes.

7.11 Are there other specific advertising practices that you wish to discuss?

Yes. From an advertising standpoint, it is crucial that all advertisements comply with Brazilian laws. In cases where individuals are featured, their prior authorization is generally required for the use of their image, name, voice, and likeness for advertising and marketing purposes. Under Brazilian legislation, these rights are considered fundamental, meaning they are inalienable and non-transferable, and can only be temporarily licensed to third parties for use in advertising campaigns.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes. International transfer of personal data is only allowed by the LGPD in the following cases:

- (a) For countries or international organizations that provide a degree of protection of personal data appropriate to the provisions of the LGPD;
- (b) When the controller offers and proves guarantees of compliance with the principles, the rights of the data subject, and the data protection regime provided for in the LGPD, in the form of: specific contractual clauses, standard contractual clauses, global corporate standards, or regularly issued stamps, certificates, and codes of conduct;
- (c) When the transfer is necessary for international legal cooperation between public intelligence, investigation, and prosecution bodies, in accordance with the instruments of international law;
- (d) When the transfer is necessary to protect the life or physical safety of the data subject or third party;
- (e) When the ANPD authorizes the transfer;
- (f) When the transfer results in a commitment made in an international cooperation agreement;
- (g) When the transfer is necessary for the execution of public policy or legal attribution of the public service;
- (h) When the data subject has given his specific and prominent consent to the transfer, with prior information on the international character of the operation, clearly distinguishing it from other purposes; or
- (i) When necessary to meet the assumptions of compliance with legal or regulatory obligation by the controller; regular exercise of rights in judicial, administrative, or arbitral proceedings; or protection of the life or physical safety of the data subject or third party.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Yes. The ANPD recently approved the new Regulation on International Transfers of Personal Data. Among the main implications arising from the Regulation are:

- (a) The criteria to be used by the ANPD to draw up this list of countries or organizations that it considers offering an equivalent level of personal data protection in line with the LGPD are described in the Regulation, also allowing the ANPD the possibility of deciding on the equivalence of standard contractual clauses from other countries;
- (b) The use of standard contractual clauses is permitted as one of the legal bases for the international transfers of personal data. In this case, processing agents must incorporate the standard contractual clauses as approved by the ANPD into their respective contractual

instruments, without any changes to the text, within a period of up to 12 months from the date of publication of the Regulation (August 23, 2024);

- (c) Data controllers may now request the ANPD to approve specific contractual clauses that offer and demonstrate guarantees of compliance with the principles, rights of the data subject, and the data protection regime as provided for in the LGPD and the Regulation; and
- (d) Data controllers may now request the ANPD to approve global corporate standards for data transfers between companies within the same group. These standards must be linked to the implementation of a privacy governance program that meets the minimum conditions established in the LGPD and the Regulation.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Brazil? Are there minimum standards? Does this differ by sector or size of the entity?

The ANPD may establish minimum technical security standards, taking into account the nature of the processed information, the specific characteristics of the processing, and the current state of technology—particularly in the case of sensitive personal data. These standards must also align with the principles set forth in the LGPD.

In October 2021, the ANPD published the ‘Guidelines on Information Security for Small-Scale Data Controllers’. The guidelines acknowledge that implementing and maintaining security measures to meet legal obligations can be complex and case-specific. In some situations, these measures may require significant investment, potentially impacting the financial capacity of small-scale data controllers. In this regard, the guidelines provide recommendations on information security measures that can help small-scale data controllers create a safer institutional environment for processing personal data. These measures focus on key areas such as policies, training, contract management, access control, data storage, communications, cloud services, and mobile devices.

9.2 How are personal data breaches regulated in Brazil? What are the requirements for notification and response?

Under the LGPD, controllers must report security incidents that pose a significant risk or harm to data subjects to both the ANPD and the affected individuals. This notification must be made within a reasonable timeframe, as defined by the ANPD, and must include at least:

- (a) a description of the nature of the affected personal data;
- (b) information about the data subjects involved;
- (c) details on the technical and security measures used to protect the data, while respecting trade and industrial secrets;
- (d) the risks related to the incident and the reasons for any delay if the notification was not immediate; and
- (e) the measures taken or planned to mitigate or reverse the effects of the incident.

The ANPD will assess the severity of the incident and may require the controller to take further actions, such as publicly disclosing the breach and implementing measures to mitigate its impact. In evaluating the seriousness of the incident, the ANPD will consider whether appropriate technical measures were in place to render the affected data unintelligible to unauthorized third parties.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The sanctions that a data controller may face from the ANPD in case of non-compliance with the provisions of the LGPD are:

- (a) warnings;
- (b) disclosure of the violation;
- (c) deletion of personal data;
- (d) simple fines of up to 2% of the gross revenue of the private legal entity, group, or conglomerate in Brazil, limited, in total, to R\$ 50 million per violation;
- (e) blockage of personal data;
- (f) suspension of some or all activities related to data processing;
- (g) suspension of the operation of the database related to the violation for up to 6 months, extendable;
- (h) suspension of data processing activities related to the violation for up to 6 months, extendable
- (i) daily fines limited to r\$ 50 million; and
- (j) damage to the company's reputation

The ANPD has been enforcing these administrative sanctions since August 2021, though it was only in 2023 that the concepts were defined more clearly for better understanding by data controllers and data subjects.

10.2 Do consumers have a private right of action? What remedies are available to them?

Individuals have a private right of action, and may bring civil and criminal lawsuits before the regular courts, under the laws referred to in question 1.2.

Lawsuits may result in compensation for material and moral damages.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement actions in privacy-related matters are evolving, and the ANPD has demonstrated its commitment to taking significant action against non-compliant practices, including those involving advertising. Some recent examples include:

- (a) In 2025, the ANPD identified potential irregularities in the use of biometric identification systems (facial recognition) for ticket sales and stadium entry across 23 football clubs. These irregularities pertain to the fulfillment of transparency obligations and the proper handling of data related to children and adolescents, as stipulated by the LGPD. As a result, the ANPD initiated inspection processes and issued a preventive measure requiring the football clubs to provide clear information on ticket sales platforms regarding the registration and biometric identification procedures for fans. Furthermore, the clubs are required to submit DPIAs related to the biometric registration and identification processes for fans and explain how the processing of biometric data of children and adolescents complies with the best interests of this vulnerable group.
- (b) In 2024, Meta's new privacy policy (covering Facebook, Messenger, and Instagram) was published, allowing the company to use publicly available information and content shared by users on its platforms to train and improve generative AI systems. This data processing could

potentially affect a substantial number of individuals, as Facebook alone has around 102 million active users in Brazil. The ANPD became aware of the situation and initiated an investigation on its own initiative, based on indications of possible violations of the LGPD. After a preliminary assessment, considering the risks of serious and irreparable harm to users, the ANPD issued a precautionary measure to suspend both the privacy policy and the data processing operation.

- (c) In 2024, the ANPD instructed TikTok to implement corrective actions and initiated an administrative sanctioning process to investigate potential irregular data processing practices involving children and adolescents. To ensure the protection of this group, the ANPD imposed the following regulatory measures on TikTok:
 - (i) complete deactivation of the 'feed without registration' feature on TikTok in Brazil within 10 business days, to ensure that children and adolescents cannot use the platform without prior registration and age verification mechanisms, given the significant risk of non-compliance with current legal standards, particularly regarding the best interests of children and adolescents;
 - (ii) the implementation of a compliance plan, to be submitted within 20 business days, aimed at improving age verification mechanisms to prevent improper registrations by children, enhancing protocols for deleting accounts belonging to this group, and establishing assistance and representation mechanisms to ensure that adolescents are assisted or represented by parents or guardians during registration.
- (d) In the realm of civil lawsuits in Brazilian courts, a notable case occurred in 2025, when the Brazilian courts sentenced Apple Computer Brasil and Google Brasil Internet for violating consumer protection and personal data protection laws. The case involved the FaceApp application, which improperly collected sensitive data from users, presented terms of use and privacy policies in foreign languages, and shared information with third parties without clear and adequate consent. The ruling mandates that both companies refrain from offering the app on their platforms until it fully complies with Brazilian legislation, particularly regarding clear information and the protection of users' personal data. The companies were also required to pay collective moral damages compensation of R\$ 19 million to the State Fund for the Protection of Diffuse Rights, as well as individual moral damages compensation of R\$ 500 to affected users.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Argentina?

Overall, cultural factors influence the acceptance of data protection mechanisms within Brazilian society. Historically, there has been a low level of trust in governmental institutions, and there is a cultural tendency to share personal information informally (eg, on social media or within close-knit groups). As a result, individuals may not always fully recognize the risks of sharing their personal data or the potential implications.

On a positive note, awareness of privacy rights has been growing in Brazil, especially following the introduction of the LGPD. However, this awareness is still developing across various sectors. Additionally, Brazil has a strong tradition of consumer protection and rights-based litigation, emphasizing the protection of individuals from unfair practices. This is reflected in the enforcement of the LGPD, allowing individuals to seek legal remedies if their data rights are violated.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

In addition to the LGPD, companies must also be aware of regulations to be issued by the ANPD (see question 11.3). To date, the ANPD has published a series of regulations, technical notes, and reports on the most diverse data privacy topics available online.

One of the key highlights is the ANPD’s decision to launch a regulatory sandbox centered on machine learning-driven artificial intelligence (‘AI’) technologies. This decision reflects the growing impact of these tools, which are already part of the daily lives of millions of people, including in Brazil. Despite their many useful applications, AI also presents significant challenges, such as the use of personal data for purposes other than initially intended, lack of transparency in automated decisions, and discriminatory biases. The ANPD recently published a technical study on Generative AI in the 3rd edition of its ‘Radar Tecnológico’ series, highlighting the risks associated with personal data usage in this context and providing key points to watch out for.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Yes. It is important for companies to stay informed about the ANPD’s regulatory agenda for the 2025-2026 period, in which important matters will be discussed and regulated. These topics include:

- Data subject rights;
- Data protection impact assessment (‘DPIA’);
- Data sharing by public authorities;
- Processing of personal data of children and adolescents;
- Sensitive personal data—biometric data;
- Security, technical, and administrative measures (including minimum technical security standards);
- Artificial Intelligence;
- High-risk personal data processing;
- Religious organizations;
- Anonymization and pseudonymization;
- Guidelines for the National Data Protection and Privacy Policy;
- Best practices and governance rules;
- Personal data aggregators;
- Sensitive personal data: health data;
- Legal basis—consent; and
- Legal basis—credit protection.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Globalization, fast tech advancements, and the boom of social media have led to a massive increase in data being created and shared everywhere. These changes in our everyday lives have also triggered major scandals, showing just how risky an unregulated digital world can be for our privacy. As a result, people have become more aware of these issues and are demanding stronger laws to protect us from the dangers lurking online.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Since the LGPD came into effect, private companies have had to adapt their operations to ensure compliance with the new legislation. To minimize risks, we recommend, for example, updating privacy policies and, when applicable, obtaining specific consent from data subjects or relying on another appropriate legal basis for processing personal data.

One of the biggest challenges for companies will be keeping up with ongoing regulatory changes. To fully comply with the LGPD and mitigate risks associated with data processing, businesses should seek guidance from specialized professionals.

12.3 What do you envision the privacy landscape will look like in five years?

In the next five years, as awareness of the importance of personal data grows and demand for government action increases, regulations are expected to become clearer and more comprehensive. This evolution will likely strengthen individuals' rights and enhance transparency in how their data is used.

 CANADA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Canada.

The Office of the Privacy Commissioner of Canada ('OPC') oversees compliance and enforces the federal privacy laws that set out the rules for the handling of personal information by federal government institutions and certain private sector businesses. It releases decisions, reports, policy statements and guidelines relating to the application and enforcement of privacy legislation. It also educates Canadians with respect to privacy rights and recourses.

Similar provincial Privacy Commissioner's offices oversee the various provincial privacy laws.

1.2 What are the primary laws regulating privacy in Canada? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

In Canada, there is both federal and provincial privacy legislation governing the collection, use, disclosure and management of personal information:

- (a) Canada has two federal privacy laws:
 - (i) the Privacy Act governs how federal government institutions deal with personal information; and
 - (ii) the Personal Information Protection and Electronic Documents Act ('PIPEDA') covers how private sector businesses collect, use and disclose personal information in the course of their commercial activities in provinces without substantially similar legislation, as well as their inter-provincial and international collection, use and disclosure of personal information. It also applies to federally regulated businesses such as banks, telecommunications companies, airlines, railways and internet service providers.
- (b) At the provincial level, Quebec, British Columbia and Alberta have enacted privacy laws deemed to be substantially similar to PIPEDA. Therefore, private sector businesses operating in those provinces may be subject to:
 - (i) the Personal Information Protection Act (British Columbia);
 - (ii) the Act Respecting the Protection of Personal Information in the Private Sector (Quebec); or
 - (iii) the Personal Information Protection Act (Alberta), rather than PIPEDA within the province (PIPEDA still applying to their inter-provincial and international activities).
- (c) In addition, certain provinces (Ontario, New Brunswick, Newfoundland and Labrador, Nova Scotia) have privacy laws in place for health information, which apply instead of PIPEDA because they have been deemed substantially similar to PIPEDA, whereas in other provinces and territories, which have also passed their own health privacy laws, PIPEDA may still apply. Certain provinces (Alberta and British Columbia) also have privacy laws that are specific to employees' personal information.

For the purposes of this chapter, we will focus on the private sector privacy legislation in (a)(ii) and (b), which we shall refer to as 'Canadian privacy legislation'.

All businesses that handle the personal information of Canadians, including for marketing and advertising purposes, need to keep these laws in mind. There is no self-regulatory body in Canada relating to privacy.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There is a limited role for self-regulation of privacy concerns in advertising practices. A key self-regulator in this area is the Digital Advertising Alliance of Canada, which is an industry self-regulatory body that establishes and enforces responsible privacy practices in the advertising industry. Its AdChoices program establishes responsible practices for online interest-based advertising, with key cornerstones including notice, transparency, and accountability from the digital advertisers.

1.4 How is privacy law enforced in Canada? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

PIPEDA is enforced by the OPC, which can launch an investigation into the business practices of companies that collect personal information, either as a result of individual complaints or as a result of its own investigations into a particular company or industry sector. The OPC also conducts audits and pursues court actions under PIPEDA, and issues reports, policy statements and guidelines.

The same is true for Alberta, Quebec and British Columbia. The regulators in these provinces are (respectively) the Office of the Information and Privacy Commissioner of Alberta, Commission d'accès à l'information du Québec and the Office of the Information and Privacy Commissioner for British Columbia.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Canada?

All private sector businesses that handle the personal information of Canadians in the course of their commercial activities are subject to PIPEDA, or the provincial privacy statutes in Quebec, Alberta or British Columbia with regards to their activities in those provinces. Quebec law also applies to non-commercial activities.

2.2 Does privacy law in Canada apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Privacy law applies to organizations conducting business in Canada that handle the personal information of people located in Canada. If a non-Canadian organization does business in Canada and collects, uses or discloses personal information of an individual in Canada, it is subject to Canadian privacy legislation, regardless of the jurisdiction in which it is located. All organizations are required to appoint a privacy officer to be responsible for compliance with Canadian privacy obligations, but that individual does not have to be located within Canada.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Canada?

The definition of ‘personal information’ in Canada is very broad and can cover most information. In short, it is information that, on its own or when combined with other information, can be used to identify an individual. In the legislation it is defined as follows:

- (a) PIPEDA: information about an identifiable individual;
- (b) Quebec: any information which relates to a natural person and directly or indirectly allows that person to be identified;
- (c) Alberta: information about an identifiable individual;
- (d) British Columbia: information about an identifiable individual, and in most cases, personal information includes employee personal information, but does not include business contact information.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

PIPEDA provides that any information can be or become sensitive, depending on the context. Certain categories of information, such as health or financial, will generally be categorized as sensitive. The OPC has also indicated that some types of information are more likely to be sensitive because they are associated with specific risks for individuals when the information is collected, used or disclosed. This information includes ethnic and racial origins, political opinions, genetic and biometric data, an individual’s sex life or sexual orientation, and religious/philosophical beliefs.

In Quebec, personal information is sensitive if, due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, it entails a high level of reasonable expectation of privacy.

‘Sensitive personal information/personal data’ is not otherwise defined in any Canadian privacy legislation.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Personal information remains regulated under private sector privacy laws if it is linked to an identifiable individual. On that basis, de-identified data that can be re-identified would still be subject to protection under data privacy laws, even while in the de-identified state. Where technology allows true anonymization of data, then it would no longer be considered (regulated) ‘personal information’.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

To comply with Canadian privacy legislation, organizations must:

- (a) post a privacy policy that explains the type of information collected, the use and any disclosure to third parties;
- (b) appoint a privacy officer: this individual would be responsible for privacy compliance and respond to any privacy complaint;

- (c) get the appropriate form of consent based on the sensitivity of the personal information and the reasonable expectations of the individual; and
- (d) maintain appropriate safeguards and notify the regulator of a data breach.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No, Canadian privacy legislation does not assign formal roles to companies based on their position relative to the personal information. The company that initially collects the personal information from the individual remains responsible for the information every step of the way, including when it is transferred to third parties for processing, as would be the case with service providers. When transferring information to a third party for processing, for example, an organization must ensure sufficient controls are in place to protect the information and otherwise comply with applicable law. For consistency with related guidance from privacy commissioners, this is typically reflected in contractual representations and warranties setting standards, handling and protection expectations, as well as granting rights to audit service providers for compliance.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Canadian privacy laws do not include the concept of lawful basis. Instead, it is structured as a consent model, which requires organizations to obtain express or implied consent to collect, use or disclose personal information (with some very limited exceptions).

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Canadian privacy laws require organizations to be transparent about their privacy practices in clear and understandable terms. While the policy should be tailored to an organization's actual practices, key topics typically include:

- (a) a description of the types of personal information collected;
- (b) the purposes for which it is used;
- (c) third party transfers and disclosure;
- (d) safeguards and retention;
- (e) individual's rights regarding their data; and
- (f) contact information for the privacy officer.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

As in most contexts, consumers have the right to informed consent for the collection and use of their personal information for advertising purposes, as well as the right to withdraw their consent for these purposes. They also have the right to understand when it is transferred or disclosed to third parties, the safeguards that will apply, the relevant retention periods that apply to their data and (in Quebec) individuals are accorded additional rights, including the right to be forgotten, data portability, and concerning automated decision making.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Consent is required for the collection, use or disclosure of all personal information, including for marketing purposes. The form of consent (express or implied) depends on the circumstances, the sensitivity of the information and the reasonable expectations of the individual. In cases where implied consent is suitable, individuals must be made aware of the marketing purposes at or before the time of collection, and in a manner that is clear and understandable (eg, just in time notices, descriptions in related privacy policies).

Individuals must be able to easily opt out of the practice; the opt out must take effect immediately and the organization must destroy or de-identify the information as soon as possible following an individual's decision to opt out.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Privacy laws in Canada do not specifically regulate vendors and other third parties involved in advertising. Organizations remain responsible for third party service providers that process personal information on their behalf, including in the context of advertising vendors.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Organizations must contractually require their vendors to comply with privacy laws when handling personal information on their behalf. This is typically structured as a data processing addendum added to service contracts, to set out the organization's specific data privacy expectations of the vendor.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

To fulfill statutory obligations under the accountability principle, organizations are expected to develop and implement a privacy management program. This program should include, for example, privacy impact assessment and threat analysis of all aspects of the organization's personal information handling practices, including ongoing activities, new initiatives, and new technologies. Measures for vendor compliance should similarly be part of an organization's ongoing due diligence, for example, including requirements that vendors processing personal information submit to compliance audits or provide third party audit reports.

In Quebec, there are statutory obligations on organizations to conduct privacy impact assessments prior to communicating personal information outside of Quebec, or undertaking a project involving the acquisition, development and redesign of an information system or electronic provision of services involving personal information.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Businesses that send emails, texts or push notifications to Canadians are subject to Canada's Anti-Spam Legislation ('CASL'). In general, to send marketing messages, businesses must have the recipient's consent (express or implied) and the message must include the prescribed disclosures, including a valid unsubscribe function.

In addition, in Quebec, marketing communications require express consent as they are considered to be a 'secondary purpose' for which consent cannot be implied.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The information collected by this technology can be classified as personal information and is subject to PIPEDA. Generally speaking, outside of Quebec, there is no automatic requirement to use cookie banners or obtain express consent to use tracking technologies. If personal information is collected, then the type of consent required (implied or express) will depend on the sensitivity of the information collected and the reasonable expectations of the individual.

In Quebec, every organization that collects personal information using technology that allows the persons concerned to be identified, located or profiled (eg, cookies and pixels), must first inform the persons that such technology is being used and must inform them of the means available to activate the functions allowing the person to be identified, located or profiled. 'Profiling' means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behavior. The regulator's position is that tracking technologies cannot be activated by default and that only the person concerned may enable it voluntarily.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions that involve personal information are subject to Canadian privacy legislation. This purpose for collecting personal information is not treated differently than other purposes. The regulation of these programs, and level of consent required, will depend on the sensitivity of the personal information collected, as well as the reasonable expectations of the individual. All purposes for which the information is collected and used will need to be disclosed clearly, for example, in the applicable privacy policy. Any purpose or use that is beyond a potential participant's reasonable expectations may require an elevated form of notice and/or express consent.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencers are not treated differently than other kinds of marketing, and influencers and organizations hosting or participating on social media platforms are subject to Canadian privacy legislation in the same manner as other organizations.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Consent is required for the collection, use or disclosure of all personal information, including for marketing purposes. See question 5.3.

In Quebec, targeted advertising requires express consent as this is considered a ‘secondary purpose’ for which consent cannot be implied. Please also see question 7.2 as targeted advertising usually implies profiling made with tracking technologies.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific privacy laws addressing digital identity resolution and clean room technologies in Canada. Uses of personal information in these contexts are subject to the same obligations regarding consent, limited use and disclosure, transparency and security as other means of processing personal information.

Some key issues arising in these contexts are data security and the practice of collecting, using or disclosing personal information beyond what is necessary for an identified purpose. Organizations should take care to ensure that only necessary information is collected, used, disclosed and retained and digital identification is not used for services that could be offered on an anonymous basis. Additionally, the security measures taken to protect personal information should be proportionate to the sensitivity of the information and digital identity ecosystems and clean rooms should be appropriately secured from unauthorized access or tampering.

In Quebec, as digital identity resolution implies that an individual has been profiled using tracking technologies, see question 7.2. It is also important to keep in mind that the definition of personal information is any information which relates to a natural person and directly or indirectly allows that person to be identified, which also includes de-identified information.

7.7 How is location-based advertising regulated under privacy law?

In Canada, there are no specific rules governing location-based advertising. Consent is required for the collection, use or disclosure of all personal information, including for marketing purposes. If location-based information is being collected and used for advertising purposes, this should be identified for individuals prior to collection (eg, in a privacy policy). To the extent that tracking technologies are used for this purpose, see question 7.2.

7.8 How are data brokers defined and regulated under privacy law?

‘Data brokers’ are not defined in Canadian privacy legislation, but the OPC has referred to data brokers using the Federal Trade Commission’s definition of ‘companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies’.

There are no specific rules governing data brokers in Canada. However, in general, any sale or other disclosure of personal information to a third party would likely require express consent from the affected individuals.

Notably, Section 7.2 of PIPEDA indicates that an organization that is a party to a prospective business transaction may disclose personal information without the knowledge or consent of the individual if the information is necessary to determine whether to proceed with the transaction and complete the transaction, and the organization receiving the information enters into an agreement requiring it to use and disclose the information solely for purposes related to the transaction, to protect the information using safeguards commensurate to the sensitivity of the information and to return the

information to the disclosing organization or destroy it if the transaction does not proceed. This exception is not available where the transaction relates specifically to the sale of personal information, however.

In Quebec, as rules about the sharing of personal information are very stringent, data brokering is likely not possible.

7.9 How is advertising to children and minors regulated under privacy law?

Given the concept of meaningful consent, the OPC takes the position that parents or legal guardians must be involved in the consent process when dealing with the personal information of children under the age of 13. In the OPC's view, this age group does not have the mental capacity or maturity to understand that nature of what they are consenting to. Individuals between 13 years and the applicable age of majority can give meaningful consent, provided the organization's privacy policy and privacy practices can easily be understood by such individuals.

In Quebec, consent from a minor under 14 years of age must be given by a person with parental authority or by a tutor (a 'tutorship' being a legal measure ordered by the courts aimed at safeguarding and preserving the assets and civil rights of a child under the age of 18 until they reach full age or they are emancipated). Consent from a minor 14 years of age or over may be given by the minor, by a person with parental authority or by a tutor. In addition, under the Consumer Protection Act (Quebec), subject to very limited exceptions, it is forbidden to make use of commercial advertising directed at children under 13 years of age.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

At this time, outside of Quebec, there are no specific rules governing profiling, the use of artificial intelligence or automated decision-making in Canada. However, when these practices involve the use of personal information, they are subject to the same obligations regarding consent, transparency and security as other uses of personal information. The federal government has also released a Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, intended to provide a framework to bridge the gap prior to specific legislation being passed.

In Quebec, every organization that uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned no later than at the time it informs the person of the decision. As this provision is very wide in scope, it also captures automated decision-making technology for advertising purposes. Please also see question 7.2 regarding profiling.

7.11 Are there other specific advertising practices that you wish to discuss?

Companies should, in order to be transparent in their handling of personal information, advise individuals that their personal information may be sent to another jurisdiction for processing or handled by third-party processor located in a foreign jurisdiction, and that it may be accessed by the courts, law enforcement and national security authorities while it is in another jurisdiction.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

- (a) Under PIPEDA, an organization is required to ‘use contractual or other means to provide a comparable level of protection while the information is being processed by a third party’.
- (b) In Alberta, under the Personal Information Protection Act (Alberta), if an organization uses a service provider outside of Canada to collect, use, disclose or store personal information, it must disclose (eg, in its privacy policy) the foreign jurisdiction in which the collection, use, disclosure or storage is taking place, and the purposes for which the information will be transferred outside Canada.
- (c) In Quebec, any organization that transfers personal information outside Quebec (including to another Canadian province) or entrusts a third party (including service providers) located outside Quebec with the task of collecting, using, communicating or keeping personal information on its behalf is required to conduct a privacy impact assessment (‘PIA’) before doing so. The PIA must take the following factors into account:
 - (a) the sensitivity of the information;
 - (b) the purpose for which the information is used;
 - (c) the protection measures, including those that are contractual, that would apply to the information; and
 - (d) the legal framework applicable in the state/province in which the information would be transferred, including the personal information protection principles applicable in that state/province.

The information may only be transferred if the PIA establishes that it would receive adequate protection, in light of generally recognized principles regarding the protection of personal information. The communication of personal information outside of Quebec must also be the subject of a written agreement that considers, in particular, the results of the PIA and, if applicable, the terms agreed upon to mitigate the risks identified in the PIA.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See question 7.11.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Canada? Are there minimum standards? Does this differ by sector or size of the entity?

There is no legislative minimum standard for securing data. All personal information must be protected by security safeguards that will ensure that the personal information is secured from theft, loss, unauthorized access, disclosure, use, copying or modification. The level of security should be commensurate to the sensitivity of the information, so the more sensitive the information, the higher the level of security. These safeguards should include physical (eg, locking filing cabinets), organizational (eg, security clearances) and technological (eg, use of encryption) measures.

In Quebec, organizations are responsible for protecting the personal information they hold. They must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

9.2 How are personal data breaches regulated in Canada? What are the requirements for notification and response?

- (a) Federally, PIPEDA requires organizations to report any breaches of security safeguards involving personal information to the Privacy Commissioner of Canada if it is 'reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual'. 'Significant harm' includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on credit record and damage to/loss of property. Factors that help determine whether a breach creates a real risk of significant harm include the sensitivity of the personal information involved and the probability that personal information has been or will be misused.

Organizations must also notify the affected individuals as soon as feasible and keep records of all breaches for at least two years. The records must include information that enables the OPC to verify compliance with reporting and notification requirements. The OPC recommends keeping records of the following information as a starting point:

- (i) date or estimated date of the breach;
 - (ii) general description of the circumstances of the breach;
 - (iii) nature of information involved in the breach; and
 - (iv) whether or not the breach was reported to the Privacy Commissioner of Canada/individuals concerned were notified.
- (b) In Alberta, organizations must report to the Office of the Information and Privacy Commissioner of Alberta any incident involving 'the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.' There is no specific timeframe for reporting prescribed; rather, the report must be provided 'without unreasonable delay'. The Office of the Information and Privacy Commissioner of Alberta may require the organization to notify individuals of the loss of their personal data, but this is not necessarily a requirement. The breach report to the Office of the Information and Privacy Commissioner of Alberta must be in writing and include information similar to that which is required by the Privacy Commissioner of Canada.
- (c) In Quebec, an organization must notify the regulator (the Commission d'accès à l'information) and the affected individuals when a confidentiality incident presents a risk of serious injury in a form that contains mandatory information. A 'confidentiality incident' means:
 - (i) access not authorized by law to personal information;
 - (ii) use not authorized by law of personal information;
 - (iii) communication not authorized by law of personal information; or
 - (iv) loss of personal information or any other breach of the protection of such information.

The ‘risk of serious injury’ assessment includes the sensitivity of the information, the anticipated consequences of its use, and the likelihood that the information will be used for injurious purposes. There is also an obligation to keep a register of breaches even if there is no risk of serious injury. In addition, in all cases, the organization must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

A Data security

- (a) Under PIPEDA, failure to comply with the breach notification provisions is an offence punishable with a fine not exceeding C\$10,000 (summary conviction) or not exceeding C\$100,000 (indictable offence).
- (b) In Alberta, failure to notify the Information and Privacy Commissioner in the event of a breach is an offence. An individual who commits an offence is liable to a fine not exceeding C\$10,000; or, in the case of a person other than an individual (eg a corporate entity), a fine not exceeding C\$100,000.

B Privacy

- (a) After receiving a complaint, the OPC can launch an investigation into a business’ privacy practices. Once the investigation is complete, the OPC will issue a report of its findings and, if applicable, offer recommendations for compliance. Further, the OPC and the business can enter into an agreement under which the business agrees to comply with the OPC’s recommendations. If the business fails to comply with the terms of the compliance agreement, the OPC can apply to the Federal Court for an order requiring the business to comply.
- (b) Beyond breach notifications, there are other statutory provisions under PIPEDA which can amount to criminal sanctions. For example, obstructing the Commissioner in the course of a complaint investigation is an offence and liable to a fine of C\$10,000 for an offence punishable on summary conviction or C\$100,000 for an indictable offence.
- (c) Similarly, in Alberta and British Columbia, commission of offences under each province’s respective privacy laws is punishable by a fine not exceeding C\$10,000 (in the case of an individual); or a fine not exceeding C\$100,000 (in the case of a person other than an individual).
- (d) In Quebec, anyone who is not compliant with privacy law commits an offence and is liable to a fine of C\$5,000 to C\$100,000 in the case of a natural person and, in all other cases, of C\$15,000 to \$25,000,000, or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. Where an offence is committed by a legal person, the administrator, director or representative of the legal person who ordered or authorized the act or omission constituting the offence, or who consented thereto, is a party to the offence and is liable to the prescribed penalty. In lieu of fines, a monetary administrative penalty may be imposed by a person designated by the regulator, on anyone who is not compliant with privacy law. The maximum possible amount of the monetary administrative penalty is C\$50,000 in the case of a natural person and, in all other cases, C\$10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under PIPEDA, within one year of receiving a Commissioner's report regarding a complaint or notice that an investigation into a complaint has been discontinued, a complainant may apply to the Federal Court for a hearing in respect of any matter in respect of which the complaint was made or that is referred to in the Commissioner's report (as long as such matter is also identified in the list of enumerated clauses set out in the Act). The court, in addition to any other remedies, may order the organization to correct its practices, publish a notice of action taken, or award damages to the complainant, including damages for humiliation.

Alberta and British Columbia's privacy statutes identify that if a person is convicted of an offence under PIPEDA, or the OPC makes an order against an organization due to a breach of PIPEDA, an individual affected by the breach or other conduct has a cause of action against the person/organization for damages suffered as result of the breach or conduct. A similar statutory cause of action is available under Ontario's Personal Health Information Protection Act 2004.

In Quebec, individuals have a private right of action (including class actions). In addition to damages and injunctive remedies, where the unlawful infringement causes an injury and the infringement is intentional or results from gross fault, the court must award punitive damages of not less than C\$1,000.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

- (a) **PIPEDA:** The federal OPC responds to complaints of PIPEDA violations from individuals or initiates its own complaints where it believes there are reasonable grounds to investigate. The OPC is required to investigate all complaints unless it is of the opinion that the complainant should first go through other review procedures, the complaint could be more appropriately dealt with through other means or the complaint was not filed within a reasonable time.

The OPC makes 'findings', but does not issue decisions regarding violations of PIPEDA. The OPC cannot order organizations to change their practices, but it may enter into compliance agreements with organizations if it finds violations of PIPEDA during an investigation. The OPC and individual complainants each have the right to bring a complaint to court.

In the advertising context in particular, we note that the Competition Bureau has begun to take enforcement action against organizations for making deceptive representations about their privacy practices. A 2020 consent agreement between the Competition Commissioner and Facebook Inc states that the respondent engaged in false or misleading advertising because it did not limit its sharing of personal information with third parties in a manner consistent with its representations to consumers and requires the respondent to pay an administrative monetary penalty in the amount of \$9,000,000.

- (b) **Competition Act:** Violations can be handled through a criminal or civil track:
- (i) Non-compliance with civil provisions prohibiting misleading advertising can result in an administrative monetary penalty up to the greater of (a) C\$10,000,000 on a first order, and C\$15,000,000 on a second order; and (b) three times the value of the benefit derived from the deceptive conduct, or if that amount cannot be easily determined, 3% of annual worldwide gross revenues. Orders can also include payment of restitution to affected parties, and the issuances of a corrective notice.
 - (ii) Conviction under the criminal offence provision prohibiting false or misleading representations can result in a fine in the discretion of the court and/or 14 years

imprisonment for indictable offences and a fine of up to C\$200,000 and/or up to 1 year of imprisonment for summary offences.

- (iii) There is also a private right of action for damages available where a misleading representation rises to the level of the criminal offence (ie, where the offence was committed knowingly or recklessly).

- (c) In **Quebec**, under guidelines published by the regulator, fines will typically only be requested (rather than monetary administrative penalties) in the most egregious cases. In addition, in accordance with these guidelines, monetary administrative penalties will not be ordered in every case of non-compliance. When a failure has occurred, a notice of non-compliance may be sent by the regulator to the organization in default to urge it to take, without delay, the measures required to remedy the failure. The notice must mention the fact that the failure could give rise to a monetary administrative penalty or penal sanctions, among other things. It is possible to enter into an undertaking with the regulator to take the measures necessary to remedy the failure or mitigate its consequences. If the undertaking is accepted by the regulator and is complied with, no monetary administrative penalty may be imposed with regard to the acts or omissions mentioned in the undertaking.

In a paper published on October 31, 2023, the Quebec regulator stated that it will continue to demonstrate proportionality in its monitoring activities, using awareness-raising when the context so requires. More recently, on January 6, 2025, the regulator's president declared that collaboration will set the tone for all the regulator's activities in 2025: 'To ensure compliance with applicable laws, we will listen to our partners and citizens. Together, we will be able to better serve the Commission's mission, which is to implement the right to information and the right to privacy.'

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Canada?

Canadian federal privacy law is often seen as a bridge between the European and US approaches to privacy. PIPEDA is focused on privacy principles as opposed to being prescriptive in its details. The goal of Canadian privacy law is to encourage compliance as opposed to being punitive in nature. It is important to note that privacy is seen as a fundamental right under Canada's Charter of Rights and Freedoms.

Quebec is the privacy leader in Canada and the concept of privacy is tied to an individual's dignity. Quebec's Charter of Human Rights and Freedoms states that every person has a right to respect of their private life. It is important to note that the Quebec Charter applies to all disputes, whether or not they involve government action. In addition, the Civil Code of Quebec states that every person has a right to the respect of their reputation and privacy.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

- (a) Alberta's Personal Information Protection Act is currently undergoing a legislative review, which is set to conclude in June 2025.
- (b) Quebec's Law 25 (previously referred to as Bill 64), an Act to modernize legislative provisions as regards the protection of personal information, received assent on September 22, 2021, and most of its provisions came into effect on September 22, 2023. Law 25's objective is to

modernize the framework applicable to the protection of personal information in Quebec, and it is now by far the most stringent privacy law in Canada.

Law 25 has introduced new rules governing the collection, use and disclosure of personal information. It requires organizations which collect personal information in Quebec to (without limitation):

- (i) obtain clear, free and informed consents which must be given for specific purposes, including express consent in some situations;
- (ii) provide mandatory information on the collection, the disclosure and other topics in clear and simple language (including by way of a privacy policy) upon collection of personal information;
- (iii) where technological means are used to identify, locate or profile individuals, provide additional information in that respect and deactivate such technology by default;
- (iv) provide privacy by default settings for technological products or services;
- (v) cease disseminating personal information and de-index any hyperlink attached to the individual's name upon a request from the individual (right to be forgotten);
- (vi) inform individuals when personal information is used to render a decision based exclusively on an automated processing of that information;
- (vii) destroy the personal information once the purpose for its collection is achieved or anonymize it, but only for legitimate purposes and in accordance with stringent technical rules;
- (viii) establish, implement and publish governance policies and practices regarding personal information as well as a privacy policy if information is collected by technological means;
- (ix) conduct PIAs of systems that handle personal information and when personal information is transferred outside Quebec;
- (x) have written agreements with all service providers and data processor that process personal information on their behalf, containing mandatory provisions;
- (xi) appoint a privacy officer and publish its title and contact information;
- (xii) dramatically limit use of biometrics; and
- (xiii) upon request, communicate computerized personal information collected from an individual in a structured, commonly used technological format (right to portability).

Since the coming into force of these new provisions, there have been relatively very few enforcement actions from the regulator or lawsuits in that respect and stakeholders are currently in a wait and see mode.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Notably, there are growing common law causes of action for invasion of privacy in some Canadian provinces (as well as a civil law cause of action in Quebec), including intrusion upon seclusion and public disclosure of private facts. Intrusion upon seclusion can be actionable if the intrusion was intentional/reckless, amounted to an unlawful invasion of the plaintiff's private affairs, and would be viewed as highly offensive to the reasonable person. Common law remedies are broad, including awards of damages and injunctive relief.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Over the past few years, Canada's privacy law landscape has undergone significant changes, with both legislative and judicial developments shaping the way businesses handle personal data. While Quebec has moved forward with comprehensive reforms, federal privacy law modernization remains stalled, creating uncertainty for organizations operating across the country. At the same time, evolving case law and increasing class action litigation are raising the stakes for businesses that fail to adequately protect sensitive information.

In particular:

- (a) Bill C-27, the Digital Charter Implementation Act 2022, was a bill set to modernize Canadian federal private sector privacy law, and included an AI-specific law, the Artificial Intelligence and Data Act. With the prorogation of Parliament, Bill C-27 died on the order paper and for that reason it is uncertain when, how, and if PIPEDA will be amended in the future.
- (b) As discussed in detail above at question 11.2(b), while federal reform is stalled, Quebec has already implemented some of the most stringent privacy laws in North America. Law 25 introduces stricter consent requirements, mandatory privacy impact assessments, and significant limitations on cross-border data transfers. Businesses transferring data outside Quebec must now conduct risk assessments and establish data transfer agreements, requirements that closely resemble the European Union's GDPR. Given these heightened obligations—and the penalties of up to 4% of global revenue for non-compliance—many companies operating across Canada are choosing to apply Quebec's higher standard nationwide rather than manage multiple privacy frameworks.
- (c) Beyond legislative developments, privacy litigation in Canada has been increasing, particularly in common law provinces. Courts have recognized new privacy torts, and class action lawsuits related to data breaches and unauthorized data collection are on the rise. As privacy class actions gain traction and regulatory enforcement powers increase, businesses must proactively strengthen their data protection measures to reduce the risk of costly litigation.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The value and quantity of personal information being exchanged, particularly across borders, has resulted in the continued rise of significant data breaches in Canada, including those involving personal financial information and personal health information. These breaches expose organizations not only to statutory risk, but, increasingly, to the risk of recourse by affected individuals. Organizations are challenged to continue to protect themselves from this risk, from threats posed by innovative technological methods of breach, as well as more long-standing risks of exposure, such as weak organizational controls and poor proactive employee training.

12.3 What do you envision the privacy landscape will look like in five years?

It is anticipated that an updated federal privacy law will come to pass over the course of the coming years, which would then likely address artificial intelligence related matters and contain increased enforcement powers for the federal commissioner, among other aspects. It is also possible that certain Canadian provinces will implement or update existing private sector privacy laws.

Additionally, common law causes of private action are becoming increasingly common, including in class actions, although there have been recent decisions in some provinces that mitigate the risk of legal action against organizations that fell victim to cybercrimes (in the absence of additional wrongdoing). Common law risk will continue to comprise a critical and increasing practical risk to organizations.

CHILE

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Chile.

In Chile, privacy is currently regulated mainly by Law No 19,628 ‘on the protection of private life’ (‘Old DPL’). The Old DPL dates from 1999, being the first Latin American regulation on the topic of personal data, and sought to regulate the market for the processing of personal data rather than to institute an autonomous right to the protection of personal data. Since 1999, the Old DPL has undergone some minor changes, which are mostly related to the transfer of debtor lists and the criteria of commercial risk assessments.

A new data protection law inspired by the GDPR, was recently approved and becomes effective on December 1, 2026 (‘New DPL’).

1.2 What are the primary laws regulating privacy in Chile? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Data protection is addressed in several specific laws, as well as provisions scattered throughout the Chilean legal framework. As well as the Old and New DPLs, data protection provisions are contained in the Constitution of the Republic of Chile, which establishes the right to ‘the respect for and protection of private life and the honor of the individual and their family, and, furthermore, the protection of personal data’. Any person who, by arbitrary or illegal act or omission, suffers a loss, perturbation or threat to this right can file a constitutional protection action. In addition, Law No 20,285 ‘on access to public information’ sets forth an individual’s right to access the information held by public administration bodies, and the procedures and exceptions thereof. Other laws contain provisions relating, inter alia, to banking, public databanks, healthcare records, and human genome data.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In regard to advertising, there is a self-regulatory body called the Association of Direct and Digital Marketing of Chile AG (‘CONAR’), which enacts the Ethics Code, which works as a non-binding ruleset of good faith practices regarding advertising in Chile.

The newest version of the Ethics Code (issued in November 2024) contains an entire chapter dedicated to the processing of personal data. The Code contains explicit provisions regarding the use of personal data in advertisements. Therefore, these rules, although voluntary, try to induce companies to honor and respect personal data when producing advertisements. Thus, we consider that it plays an educational role in the sense of teaching companies the ethical importance of personal data, which sort of complements the legal obligations of honoring them set forth by the DPL.

1.4 How is privacy law enforced in Chile? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

We must make a distinction between the law before and after the coming into force of the New DPL on December 1, 2026:

(a) **Pre-December 1, 20226**

- (i) The remedy set out in the Old DPL is the habeas data action, by means of which individuals may request a civil tribunal to enforce their data protection rights in the event of a breach by a specific data controller. This habeas data action follows a summary proceeding. Should the claim be accepted, the civil tribunal will set a reasonable period of time to comply with the decision and may apply fines of up to 50 monthly tax units (approx USD 3,500).
- (ii) Moreover, the controller must compensate for the patrimonial and moral damage caused by the improper processing of data, without prejudice to proceedings to erase, modify or block data as requested by the individual concerned, or as ordered by the civil tribunal, as the case may be. This action for damages may be filed together with the habeas data action. In these cases, the amount of compensation will be established by the judge, considering the circumstances of the case and the seriousness of the facts. Case law has established compensation for moral damages to data subjects in amounts of approx USD 6,000.
- (iii) However, those who are victims of an illegitimate processing of their data rarely execute the habeas data action, and instead choose to proceed through the constitutional protection action, which is characterized by its speed and low cost. Through it, any person can request a Court of Appeal to take measures to bring to an end an arbitrary or illegal act or omission, namely a deprivation, disturbance or threat to their constitutional rights and guarantees (one of which being the right to data protection and privacy).
- (iv) Regarding public data processing, Law No 20,285 granted the Chilean Council for Transparency the competence to ensure adequate compliance with the Old DPL regarding the protection of personal data by the organs of the state administration.
- (v) Also, under the Consumer Protection Law, the national consumer service ('SERNAC') has the duty to ensure the proper treatment of consumers' personal data in the context of consumer relations.

(b) **December 1, 2026 onwards**

- (i) Once the new DPL comes into force, while the habeas data action remains, the new regulation sets forth the Data Protection Agency ('Agency'), which will have a regulatory/inspection role, and creates a sanctioning procedure to be conducted before the Agency. Therefore, the enforcement of the New DPL will mostly be through the way of sanctioning procedures before the Agency, who can impose high fines (up to approx USD 1,4 M), depending on the nature of the infringement.
The Agency may commence the proceedings ex officio or through a complaint filed by a third party.
- (ii) Furthermore, as mentioned in the answer to question 1.3, the advertising self-regulator, CONAR, also operates as a non-binding 'court' where third parties can denounce and ad if it breaches the Ethics Code's provisions on data protection, and CONAR may order the removal of said ad.

Note that, if an ad breaches the Ethics Code, it will probably breach the provisions of the New DPL, so a double proceeding could take place: one before CONAR for breach of the Ethics Code and another before the Agency for infringement of the New DPL.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Chile?

Under the New DPL, a company becomes subject to the law if:

- (a) it processes personal data (either directly as a data controller or indirectly as a data processor) and said company is based in Chile.
- (b) if the processor is not located in Chile, the law will still apply to it if:
 - (i) the controller on whose behalf it operates is based in Chile.
 - (ii) if the controller and processor are not based in Chile, if the processing relates to the offering of goods or services to data subjects in Chile.
- (c) the parties to an agreement decide to have Chilean law as the applicable legislation governing said agreement.

2.2 Does privacy law in Chile apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

See question 2.1.

Foreign companies are required to maintain an official email address to which the Data Protection Agency may send notices and communications. This same mail shall also be used by data subjects who wish to exercise their rights against the company.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Chile?

- (a) **The Old DPL:** defines personal data as ‘any data related to information of any type concerning identified or identifiable natural persons’.
- (b) **The New DPL:** defines it as ‘any information linked or referable to an identified or identifiable natural person. An identifiable person shall be understood as any individual whose identity can be determined, directly or indirectly, in particular by reference to one or more identifiers such as name, national identification number, or the analysis of elements specific to that person’s physical, physiological, genetic, mental, economic, cultural, or social identity’.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

- (a) **The Old DPL:** defines sensitive data as ‘personal data that refers to any physical or moral characteristics of any person, or to facts or circumstances of his or her intimate sphere, such as personal habits, racial origin, political ideologies and opinions, religious beliefs, physical and mental health, and sexual life’. It is a broad definition which has to be interpreted to include new type of data, such as biometric data, which were not commonly available at the time that the Old DPL was drafted.
Sensitive data may not be processed unless:
 - (i) there is legal authorization,
 - (ii) the data subject has consented, or
 - (iii) the sensitive data is necessary to grant healthcare benefits to its holder.

- (b) **The New DPL:** defines it as ‘Personal data shall be deemed to have this status when they refer to an individual’s physical or moral characteristics, or to facts or circumstances pertaining to their private life or intimacy, and which reveal ethnic or racial origin, political, trade union or professional association affiliation, socioeconomic status, ideological or philosophical convictions, religious beliefs, health data, human biological profile, biometric data, and information relating to the natural person’s sex life, sexual orientation, or gender identity’.

Sensitive data are regulated differently, as they are subject to a more stringent standard due to their nature, and therefore, the legal bases for their processing are significantly limited. Generally speaking, they may only be processed with the data subject’s explicit consent, and exceptionally, other legal grounds are permitted, which are as follows:

- (i) When the processing concerns sensitive personal data that the data subject has manifestly made public, and such processing is related to the purposes for which the data were made public;
- (ii) When the processing is based on a legitimate interest pursued by a legal entity governed by public or private law that does not operate for profit, and the following conditions are met:
 - its purpose is political, philosophical, religious, cultural, trade union, or professional association-related;
 - the processing is carried out exclusively with respect to its members or affiliates;
 - the data processing is aimed at fulfilling the specific purposes of the institution;
 - the legal entity provides adequate safeguards to prevent data breaches, theft, or unauthorized use or processing of the data; and
 - the personal data are not communicated or transferred to third parties.Where these conditions are met, the legal entity does not require the data subject’s consent to process their data, including sensitive personal data. In the event of doubt or in any administrative or judicial dispute, the data controller must demonstrate compliance with these requirements.

When a data subject ceases to belong to the legal entity, their personal data must be anonymized or deleted.
- (iii) When the processing of the data subject’s personal data is indispensable for safeguarding the life, health, or physical or psychological integrity of the data subject or of another person, and when the data subject is physically or legally unable to provide consent. Once the impediment ceases, the controller must provide the data subject with detailed information regarding the data that were processed and the specific processing operations carried out;
- (iv) When the processing of data is necessary for the establishment, exercise, or defense of a legal claim before judicial or administrative authorities;
- (v) When the processing of data is necessary for the exercise of rights or the fulfillment of obligations of the controller or the data subject, in the context of employment or social security, and is carried out in accordance with applicable law; or
- (vi) When the processing of sensitive personal data is expressly authorized or mandated by law.

Furthermore, when the legal grounds other than consent are invoked, a prior, mandatory data protection impact assessment (‘DPIA’) must be conducted.

Finally, it should be noted that some of the categories that fall under the definition of sensitive data have even stricter regulations for their processing and the legal basis that may be invoked.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

- (a) **The Old DPL** does not contemplate this.
- (b) Under **the New DPL**:
 - (i) **Anonymized data** ceases to be regarded as personal data (because it is not possible to identify a person through it), and thus personal data falls out of the scope of the law once it is anonymized;
 - (ii) **Pseudonymized data** remains as personal data, as it is possible to match the original data subject to the pseudonym. The law regards pseudonymization as one of the security measures that data controllers and data processors can implement, provided that the way for matching the pseudonym with the data subject is kept hidden/secret with only few people having access to it. Therefore, it will be regarded as one of the effective ways to comply with the security obligations imposed by the New DPL.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The essential obligations are to comply with the different principles of the law, which are the following (we must note that, although the principles were ‘implied’ in the Old DPL, and recognized by legal doctrine, the New DPL expressly includes them, being regarded as enforceable obligations):

- (a) **Principle of Lawfulness and Fairness:** Personal data may only be processed in a lawful and fair manner. The data controller must be able to demonstrate the lawfulness of the personal data processing it carries out.
- (b) **Principle of Purpose Limitation:** Personal data must be collected for specific, explicit, and lawful purposes. The processing of personal data must be limited to achieving such purposes. In accordance with this principle, personal data may not be processed for purposes other than those communicated at the time of collection, unless the processing is for purposes compatible with those originally authorized; there is a contractual or pre-contractual relationship between the data subject and the data controller that justifies processing for a different purpose, provided such purpose falls within the scope of the contract or is consistent with the negotiations or arrangements prior to its conclusion; the data subject grants renewed consent; or the law so provides.
- (c) **Principle of Proportionality:** Personal data processing must be strictly limited to data that are necessary, adequate, and relevant in relation to the purposes of the processing. Personal data may only be retained for as long as necessary to fulfill the purposes of the processing, after which they must be deleted or anonymized, without prejudice to any legal exceptions. A longer retention period requires either a legal authorization or the consent of the data subject.
- (d) **Principle of Data Quality:** Personal data must be accurate, complete, up-to-date, and relevant in relation to their source and the purposes of the processing.

- (e) **Principle of Accountability:** Those who process personal data shall be legally responsible for complying with the principles set forth in this Article, as well as with the obligations and duties established by law.
- (f) **Principle of Security:** In processing personal data, the data controller must ensure appropriate security standards, protecting the data from unauthorized or unlawful processing, as well as from loss, leakage, accidental damage, or destruction. Security measures must be appropriate and proportionate to the nature of the processing and to the sensitivity of the data.
- (g) **Principle of Transparency and Information:** The data controller must provide the data subject with all information necessary for the exercise of the rights established under this law, including its policies and practices regarding personal data processing, which must also remain permanently accessible and available to any interested party in a precise, clear, unambiguous, and free manner. The data controller must take appropriate and timely measures to facilitate the data subject's access to all information provided for under this law, as well as to any other communication related to the processing carried out.
- (h) **Principle of Confidentiality:** The data controller and any person who has access to personal data must maintain confidentiality or secrecy in relation to such data. The controller shall establish appropriate controls and measures to preserve confidentiality. This duty shall remain in force even after the relationship with the data subject has ended.

All the obligations set forth by the New DPL and its complementary regulations derive from, or constitute concrete manifestations of these principles, and any violation of these principles shall constitute an infringement.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

Yes, the New DPL expressly regulates the roles of data controller (the person who determines the purposes and means of the processing) and data processor (the person who carries out the processing of data under the instructions and on behalf of the controller).

While the controller is subject to all the obligations and duties imposed by the law, the processor is only responsible for fulfilling two main obligations: the duty to implement security measures and the duty to maintain confidentiality.

4.3 **Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

Yes, the New DPL expressly regulates the legal bases for processing personal data and sets forth that personal data may not be processed unless there is a lawful basis supporting such processing. Notwithstanding the special regulation applicable to certain categories of data (such as sensitive data: see question 3.2), the law recognizes the following general legal bases for processing:

The general rule is the data subject's consent, which, as stated elsewhere, must be freely given and actively expressed through a positive act.

Additionally, the processing of personal data without the data subject's consent is permitted in the following cases:

- (a) When the processing refers to data concerning financial, banking, commercial, or economic obligations, and is carried out in accordance with the legal provisions applicable to such matters, including data related to the data subject's socioeconomic status;
- (b) When the processing is necessary for the performance or fulfillment of a legal obligation, or when mandated by law;
- (c) When the processing is necessary for the conclusion or performance of a contract between the data subject and the controller, or for the implementation of pre-contractual measures taken at the request of the data subject;
- (d) When the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, provided that such interests do not override the rights and freedoms of the data subject. In any event, the data subject shall always have the right to be informed about the processing and the legitimate interest on which it is based; or
- (e) When the processing is necessary for the granting, exercise, or defense of legal claims before courts of law or public authorities.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

There are no specific requirements for the contents of the privacy notices for advertising purposes, so the general requirements apply. Therefore, the privacy notice must at least disclose:

- (a) the identity of the data controller,
- (b) whether it uses data processors (and their identity),
- (c) what personal data it collects and how it is used,
- (d) the legal basis for the processing,
- (e) the purposes of the processing and
- (f) the email or contact information on how data subjects may exercise their rights.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have all 6 privacy rights allocated to data subjects by the new privacy law, namely the rights of:

- (a) access,
- (b) rectification,
- (c) erasure,
- (d) restriction of processing,
- (e) data portability, and
- (f) the right to object.

Obviously, the practical use of each of these rights will depend on the context and nature of the advertising.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

If the advertising activities include the processing of personal data (such as the sending of marketing emails) then consent from the data subject must be collected (unless another legal basis can be invoked, which may be complicated). The New DPL states that the data subject's consent to processing must be freely given, and specific as to its purpose or purposes, and that the data subject must be informed of the purpose of the processing. Furthermore, consent has to be expressed in advance and in an unambiguous manner, by means of a verbal or written declaration, through an equivalent electronic means, or by an affirmative act that clearly indicates the data subject's will.

Furthermore, the law states that the data subject may revoke the consent granted at any time and without the need to state a reason, using means that are similar or equivalent to those employed for the granting of consent. The means used for granting or revoking consent must be expeditious, reliable, free of charge, and permanently available to the data subject. The revocation of consent has no retroactive effect.

Thus, opt-out options must always be provided, and must be as easy to use by the data subject as the opt-in mechanism for granting consent.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

There are no regulations regarding this.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

If it is done in the context of a relationship between a data controller and a data processor, then a data protection agreement ('DPA') is required. The New DPL states that the DPA must specify:

- (a) the subject matter of the processing;
- (b) its duration;
- (c) the purpose of the processing;
- (d) the type of personal data processed,
- (e) the categories of data subjects concerned; and
- (f) the rights and obligations of the parties.

So, the actual obligations are not legally defined but rather it is left as a matter to be determined by the parties.

The Agency will make model contract templates available to the public on its website.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

It is expected that companies will conduct a 'Privacy Due Diligence' and review and assess whether the party with which they are about to engage in commercial operations complies with all the regulations set forth by the new privacy law, as well as with the 'good practices' associated with the particular industry/business.

There are no specific regulations regarding impact assessments for advertising purposes. However, there are indeed instances where the law requires conducting a mandatory DPIA, so if such processing is conducted for advertising purposes, then it could be said that a DPIA is conducted for advertising purposes.

The New DPL requires a mandatory DPIA when it is likely that a type of data processing, by virtue of its nature, scope, context, technology used, or purposes, may result in a high risk to the rights of the data subjects.

In addition, a DPIA is always required in the following cases:

- (a) a systematic and comprehensive evaluation of personal aspects relating to data subjects, based on automated processing or decision-making, such as profiling, that produces legal effects or similarly significant consequences for the data subjects;
- (b) large-scale or massive processing of personal data;
- (c) processing that involves systematic observation or monitoring of a publicly accessible area; or
- (d) processing of sensitive or specially protected personal data, in cases where the legal basis for processing is not the consent of the data subjects.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.4 How is social media and influencer marketing regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are no specific regulations, either in the Old DPL or the New DPL.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.7 How is location-based advertising regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL.

7.9 How is advertising to children and minors regulated under privacy law?

There are no specific regulations, either in the Old DPL or the New DPL. There is a specific regulation for the processing of personal data related to children, but it makes no reference to advertising.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific regulations for advertising purposes. There is a 'general' regulation which deals with the processing of personal data through automated decision-making technology, which it considers to be a 'risky action' and thus be subject to a mandatory DPIA.

7.11 Are there other specific advertising practices that you wish to discuss?

No. In general we can say that the privacy law does not regulate anything related to advertising. The only specific regulation related to advertising and personal data is the Ethics Code.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The New DPL expressly regulates the international transfer of personal data, establishing that such transfer is lawful in the following cases:

- (i) When the transfer is made to a person, entity, or public or private organization subject to the legal system of a country that ensures an adequate level of personal data protection (the Agency shall issue a list of countries that meet this standard).
- (ii) When the data transfer is covered by contractual clauses, binding corporate rules, or other legal instruments entered into between the data controller initiating the transfer and the receiving controller or third-party processor, and such instruments provide adequate safeguards as defined by law.
- (iii) When the data controller initiating the transfer and the receiving controller or third-party processor adopt a compliance model or certification mechanism that includes adequate safeguards as defined by law.

In the absence of an adequacy decision or adequate safeguards, a specific and non-repetitive transfer may take place if one of the following conditions is met:

- (a) when the data subject has given explicit consent to a specific and clearly defined international data transfer;
- (b) when the transfer concerns specific banking, financial, or securities transactions carried out in accordance with the laws governing such transfers;
- (c) when the data must be transferred in order to fulfill obligations arising from treaties or international agreements ratified by the Chilean State and currently in force;
- (d) when the transfer is necessary for the application of cooperation agreements, information exchange, or supervision arrangements entered into by public bodies in the performance of their duties and within the scope of their legal authority;
- (e) when the transfer of data by a natural or legal person, whether public or private, has been expressly authorized by law and for a specific purpose;

- (f) when the transfer is carried out for the purpose of providing or requesting international judicial cooperation;
- (g) when the transfer is necessary for the conclusion or performance of a contract between the data subject and the controller, or for the implementation of pre-contractual measures taken at the request of the data subject; and
- (h) when it is necessary to adopt urgent medical or healthcare measures for the prevention or diagnosis of diseases, for medical treatment, or for the management of healthcare or health services.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Chile? Are there minimum standards? Does this differ by sector or size of the entity?

The New DPL sets forth the obligations of both data controllers and data processors to adopt ‘security measures’ in their processing activities (ie, encryption, passwords, etc). As a general principle, the standard is set by the size of the company: small businesses are subject to a lower threshold than that imposed on large corporations. Similarly, the standard also differs depending on the nature of the data being processed (ie, the processing of sensitive data (such as that a person is suffering from a particular disease) shall bear a higher standard than the processing of ‘regular’ personal data (such as a person’s name).

9.2 How are personal data breaches regulated in Chile? What are the requirements for notification and response?

The New DPL places an obligation on data controllers to report to the Data Protection Agency any data breach/incident that occurs in relation to the personal data that they process that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed, when there is a reasonable risk to the rights and freedoms of the data subjects. The data controller must document such communications, describing:

- (a) the nature of the breaches suffered,
- (b) their effects,
- (c) the categories of data involved,
- (d) the approximate number of affected data subjects, and
- (e) the measures taken to address the breaches and prevent future incidents.

Where such breaches concern sensitive personal data, data relating to children under the age of fourteen, or data concerning economic, financial, banking, or commercial obligations, the controller must also notify the data subjects, or their legal representatives where applicable. This notification must be provided in clear and plain language, specifying the data affected, the potential consequences of the security breaches, and the remedial or protective measures adopted. Notification must be made to each affected data subject individually. If individual notification is not possible, a public notice shall be issued through a mass media outlet with nationwide reach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) The Old DPL sets forth no penalties.
- (b) Conversely, the new privacy law sets forth a series of infringements/offenses that are classified as ‘minor’, ‘serious’ or ‘gross/very serious’, with the penalties being fines, whose amount will depend on the seriousness of the offense:
 - (i) Minor infractions: fine of up to USD 375,000.
 - (ii) Serious infractions: fine of up to USD 750,000.
 - (iii) Gross infractions: fine of up to USD 1,500,000.

In the event that fines are imposed for repeated very serious infringements within a 24-month period, the Agency may order the suspension of data processing operations and activities carried out by the data controller, for a period of up to 30 days.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, as mentioned previously:

- (a) Under the Old DPL data subjects can file the ‘habeas data’ action as well as filing a constitutional protection action.
- (b) Under the New DPL, data subjects can file an infringement claim before the Agency and seek the imposition of fines on an infringing data controller (or data processor, in some cases). Furthermore, data subjects may file a civil lawsuit against an infringing data controller (or data processor, in some cases) and seek damages to compensate for losses experienced by the data subject due to the breach of the law (eg, if a data controller conducted processing of the subject’s personal data without a legal basis).

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Given that the Data Protection Agency is created by the New DPL, which has yet to become effective, there is no actual ‘enforcer’ for the time being, and thus, no enforcement has been carried out in any matters regarding data protection (let alone data protection in the context of advertising).

As for CONAR, the provisions relating to the processing of personal data were only recently incorporated in the newest version of the Ethic Codes which became effective in early 2025; and, as of the current date, we have found no cases related to the breach of these provisions.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Chile?

The truth is that, to this day, there is not a strong data protection culture in Chile. It is common for many types of personal data to be easily accessible and routinely ‘traded’ as if it were of little consequence. For example, individuals’ national identification numbers are frequently requested by commercial establishments, and people usually provide them without much concern. The New DPL is expected to change this reality; however, it is anticipated that it will take time for both individuals and companies in Chile to shift their mindset accordingly.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

As we have mentioned in other responses, the main challenge lies in ensuring that companies in Chile fully understand the significance of the new regulation and adopt a true ‘corporate culture’ of data protection. This involves recognizing the importance of data processing and of working toward the elimination of certain common practices that are inconsistent with the principles established by the law—such as the widespread custom of routinely requesting individuals’ national identification numbers in many commercial transactions where it is not essential.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The most important thing is for companies to fully appreciate the weight of the law and to take advantage of the ‘grace period’ prior to the entry into force of the New DPL to shift their corporate mindset and implement a comprehensive culture of compliance and respect for the protection of personal data

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Well, the obvious main change is the approval of the New DPL that becomes effective on December 1, 2026. The New DPL was passed because the old (still current) law dated from the year 1999, and, while it was innovative at the time, it has become outdated and out of touch with current technology and with the current international standards of data privacy.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenge is, without a doubt, the implementation of the New DPL, where companies have a two-year ‘grace period’ to adapt to the new regulations and install corresponding technological and legal measures to ensure compliance with the New DPL. Many companies still struggle to understand the relevance of data privacy and the considerable sanctions that the New DPL will apply to infringements.

12.3 What do you envision the privacy landscape will look like in five years?

Hopefully in five years’ time the landscape will have changed considerably, with most companies having adopted robust data protection policies, and, equally as important, with a ‘change of mind’ whereby personal data is really treated as a sensible and confidential issue and not just as an ‘asset’ that can be freely used and collected. Unfortunately, we consider that only some companies will really take this into account and the rest will feel ‘obliged’ to comply once the Data Protection Agency starts conducting sanctioning proceedings and imposes fines.

CHINA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in China.

China data regulation essentially began in 2017 with the Cybersecurity Law ('CSL'), which established security requirements for network operators, restrictions on cross-border data transfers, and also generally called for data security and personal information ('PI') protection in China, but did not provide many details. At the end of 2021, those details finally emerged in the form of the groundbreaking Data Security Law ('DSL') and Personal Information Protection Law ('PIPL'). These three laws are now the three pillars of the Chinese data protection legislation system and together form an overarching framework governing data processing and cybersecurity issues relevant to China, including strict restrictions and obligations similar to what is seen in other advanced economies. In addition, the Regulations on Network Data Security Management released in 2024 provide detailed operational guidelines for the implementation of the three fundamental data laws. The Chinese Civil Code now also includes a right of privacy.

1.2 What are the primary laws regulating privacy in China? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) **CSL:** The CSL provides various security protection obligations for network operators (a very broad category encompassing nearly any company that operates an internet-enabled business, platform or interface), and imposes a series of heightened security obligations for critical information infrastructure (CII) operators ('CIIOs'). 'CII' refers to information infrastructure used for public communications and information services, energy, transport, water conservancy, finance, public services, e-government affairs or other important industries and fields, or other information infrastructure that will result in serious damage to national security, the national economy or the public interest if destroyed or damaged, or suffering a data leak. These heightened security obligations include the protection of PI, as addressed further below.
- (b) **DSL:** The DSL establishes basic systems for classified and graded data management, data security risk assessment, monitoring and early warning requirements, emergency responses and data security review ('System'). It also provides a definition for data, which includes any record of information in electronic or other forms.
- (c) **PIPL:** The PIPL specifically regulates the processing of PI, including collection, storage, use, processing, transmission, provision, disclosure, and deletion. The PIPL draws inspiration from the GDPR, but has unique characteristics responsive to Chinese priorities. Similar to the GDPR, the impact of the PIPL has been significant, bringing coherence to the regulation of PI in China, but also substantially increasing the requirements, restrictions, and potential liabilities that personal information processors ('PI processors') may face, including those operating outside of China—please refer question 2.2.
- (d) **Civil Code:** The Civil Code includes many provisions that specifically or generally relate to the protection of personal data. For example, it sets out a 'right of privacy' as one of the 12 types of 'civil rights and interests' protected under the Law. Under the Civil Code, violation of the right of privacy and related infringement of PI rights is clearly identified as a tort.

- (e) **Criminal Law:** The Criminal Law can apply where any individual (including staff of governmental authorities and companies engaged in various industrial sectors, including finance, telecommunications, transportation, education and healthcare) sells or illegally provides PI obtained in the course of their employment. It is also may be applicable if an individual illegally acquires such information by theft or by any other means. The legal consequences of such acts can include fixed-term imprisonment of up to three years (up to seven years where the circumstances are ‘serious’), criminal detention, or fines.
- (f) **Regulations on Network Data Security Management:** These regulations provide comprehensive implementing rules for the CSL, DSL, and PIPL, including requirements for network data security, PI protection, and the management of important data. In addition, these regulations stipulate obligations for internet platform service providers.
- (g) Various governmental authorities at the central level have also issued administrative regulations to set out more specific requirements in their areas and to provide rules for different types of PI. Local governmental authorities have also issued privacy-related administrative regulations for their jurisdictions.
- (h) Finally, there are also national standards, many of which are not explicitly binding, but will be referenced by the authorities when making investigation and enforcement decisions. In particular, the Information Security Technology—Personal Information Security Specification (GB/T 35273-2020,) (‘**2020 Specification**’). Before the PIPL, the 2020 Specification was the most comprehensive general PI management guidance applicable in China. It has been largely superseded by the PIPL, but is still widely referred to, particularly where it provides standards on issues that are not covered in detail under the PIPL.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays a moderate role. Industry self-regulation bodies are supported by the state to develop codes of conduct, strengthen industry self-regulation, and promote the healthy development of the industry. There are many self-regulation bodies in China that are relevant to data and advertising, such as the China Consumer Association (‘CCA’), the China Advertising Association, the Cyber Security Association of China (‘CSAC’), and the Internet Society of China (‘ISC’). These play a mostly supporting role in privacy regulation.

1.4 How is privacy law enforced in China? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Breaches of privacy obligations can lead to administrative penalties, including rectification orders and significant fines (See question 10), as well as civil litigation, and criminal liability in serious cases. Administrative enforcement actions often come in the form of sector-specific campaigns, such as those targeting apps for illegally collecting or using user data, which have resulted in many apps changing their data practices, being fined or being de-listed. Large platforms and tech conglomerates are also under continuous scrutiny. In addition, the people’s procuratorates at all levels are authorized to initiate civil and administrative public interest litigation on PI protection issues, and the Supreme People’s Procuratorate has already published several sample cases of this type of public interest litigation. Private individuals can also bring claims for infringement of privacy rights under the Civil Code, PIPL, and related laws for enforcement through the courts, and this is becoming more common as China’s privacy laws mature.

Key authorities for privacy-related matters include:

- (a) **The CAC:** responsible for the planning and coordination of cybersecurity and related matters, including PI protection, along with other authorities;
- (b) **The MIIT:** responsible for supervision and administration of PI in the telecommunications and internet sector;
- (c) **The MPS:** with general authority over all criminal matters, including with respect to the unlawful obtaining, sale or disclosure of PI and other privacy-related infractions;
- (d) **The SAMR:** responsible for implementing the law in the marketing sector;
- (e) **The CCA:** a government-connected industry self-regulation organization, which accepts and handles certain consumer complaints (including referral to other authorities where warranted) and sometimes undertakes coordinated campaigns.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in China?

All companies that have operations related to China or that process Chinese-origin data (regardless of whether they have operations or entities in China) are potentially subject to Chinese laws relating to privacy and PI. For example, the PIPL claims substantial extraterritorial jurisdiction—it not only applies to PI processing carried out within China, but also to processing done outside of China where the purpose of the processing is to provide products or services to Chinese natural persons, or to evaluate their behavior. Similarly, the DSL not only applies to data processing activities conducted within the territory of China, but also claims extraterritorial application to data processing activities conducted outside of China that may harm national security, the public interest or the legitimate rights and interests of Chinese citizens and organizations. All companies and their employees in China are generally subject to the Criminal Law and the Civil Code. In addition, any ‘network operator’ (which is a very broad category encompassing nearly any company that operates an internet-enabled business, platform or interface) is further subject to the personal data protection measures under the CSL and all of its related implementing regulations.

2.2 Does privacy law in China apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, please refer to question 2.1. Companies outside of China engaged in certain China-related data processing may be obligated to set up a dedicated office or appoint a designated representative within the territory of the China to be responsible for PI protection-related affairs, and submit the name of such office or the name and contact information of the representative to the authorities (ie, the local branch of the CAC at the municipal level).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in China?

The most definitive definition so far comes from the PIPL, which identifies ‘PI’ as any kind of information related to identified or identifiable natural persons, electronically or otherwise recorded (excluding anonymized information).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Under the PIPL, ‘sensitive PI’ is defined as PI that, once leaked or illegally used, will easily lead to infringement of human dignity or harm to the personal safety or property of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal location tracking and other information of a natural person, as well as any PI of a minor under the age of 14.

Sensitive PI is subject to more restrictions. PI processors may only process sensitive PI with separate (unbundled) consent, which includes notification to the PI subject of the need for such processing and the potential impact on the individual’s rights and interests. Processing the PI of minors under the age of 14 requires parental consent and specific PI processing rules. In addition, the processing of sensitive PI must have a specified purpose, sufficient necessity for the processing, and strict protection measures, including the requirement that the PI processor must conduct a PI protection impact assessment.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under the PIPL, ‘anonymization’ refers to the process by which any PI is processed to the extent that it cannot identify a specific natural person and cannot be restored to its original state. Accordingly, anonymized data is no longer deemed to be PI, and therefore the processing of anonymized data is not subject to the rules of the PIPL. In contrast, de-identification or pseudonymization refers to the situation where PI is processed to the extent that it cannot identify a specific natural person without the help of additional information. Such PI is still deemed to be PI, which means the processing of such information is still subject to the rules under the PIPL.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

In brief, the key obligations include the following:

- (a) PI processing must have lawful basis. Please refer to question 4.3;
- (b) PI must be processed in accordance with the principles of openness and transparency, with the rules for the processing of PI disclosed;
- (c) Processing of PI must be for a specified and reasonable purpose, and be conducted for a purpose directly relevant to the disclosed purpose of processing and in a way that has the least impact on personal rights and interests. Collection of PI must be limited to the minimum scope necessary for achieving the purpose of the processing and shall not be excessive;
- (d) The retention period for PI shall be the minimum period necessary for achieving the purpose of processing, unless any law or administrative regulation stipulates otherwise;
- (e) The quality of PI must be ensured when the PI is processed in order to avoid any negative impact on personal rights and interests due to any inaccuracy or incompleteness of the personal information processed; and
- (f) PI processors are responsible for their PI processing activities, and must take measures necessary to ensure the security of the processed PI.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. The PIPL defines a **PI processor** as ‘any organization or individual that independently determines the purpose and method of processing in their activities of processing of PI’. This generally correlates with the role of data controller under GDPR. PIPL uses the term ‘**entrusted party**’ to refer to a party accepting a processing request from a PI processor to process PI as instructed by such PI processor. This role would be called a data processor under the GDPR.

Most privacy compliance obligations fall to the PI processor, with the entrusted party mostly having obligations related to PI security and supporting the PI processor’s compliance activities.

The PIPL also has a joint-controller concept (similar to the GDPR), stipulating that two or more PI processors who jointly decide on the purpose and method of the PI processing shall set out their respective rights and obligations in a joint processing agreement, which must not compromise the right of data subjects to exercise their rights as provided for under law. The joint processors will be held jointly and severally liable for any damages caused by an infringement of personal rights and interests.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, PI processing must meet one of the following lawful bases:

- (a) Where consent is obtained from the individual;
- (b) Where it is necessary for the conclusion or performance of a contract to which the individual is a contracting party, or where it is necessary for carrying out human resources management under an employment policy legally established or a collective contract legally concluded;
- (c) Where it is necessary for performing a statutory responsibility or statutory obligation;
- (d) Where it is necessary for responding to a public health emergency, or for protecting the life, health or property safety of the natural person in the case of an emergency;
- (e) Where the PI is processed within a reasonable scope to carry out any news reporting, supervision by public opinions or any other activity for public interest purposes;
- (f) Where the PI, which has already been disclosed by the individual or otherwise legally disclosed, is processed within a reasonable scope and in accordance with the law; or
- (g) Any other circumstance as provided by law or administrative regulations.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

In brief, the privacy notice shall at least include the following:

- (a) The name and contact information of the PI processor;
- (b) The purpose, method, and type of PI being processed, the necessity of processing sensitive PI, and the impact on individuals’ rights and interests;
- (c) The retention period for the PI, and the method of processing after the expiration of the retention period (if it is difficult to determine the specific retention period, the method of determining the retention period shall be specified);

- (d) Methods and channels for individuals to access, copy, transfer, correct, supplement, delete, and restrict the processing of PI, to cancel their accounts and withdraw their consent;
- (e) When providing PI to other PI processors, the PI processor shall disclose the name and contact information of the receiving party, the purpose and method of the processing, and the type of PI involved. Note that this is often done at a separate URL that can be periodically updated;
- (f) For outbound transfer of PI, the PI processor shall disclose the name and contact information of the overseas recipient, the purpose and method of the processing, and the type of PI involved, as well as the method for the individual to exercise his/her rights against the overseas recipient;
- (g) When processing PI of minors under the age of 14, the PI processor must establish special PI processing rules for minors following the various requirements for such processing (see question 7.9).

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Under the PIPL, CSL and the 2020 Specification, individuals have the following key rights in relation to the processing of their PI in advertising contexts:

- (a) Right to know of processing, and have access to and receive copies of processed PI;
- (b) Right to correct or complete their PI;
- (c) Right to delete data under certain circumstance;
- (d) Right to object to, or to restrict, processing;
- (e) Right to data portability under certain circumstance;
- (f) Right to withdraw consent;
- (g) Right to complain to the relevant data protection authorities;
- (h) Right to require PI processors to explain their rules for PI processing; and
- (i) Right to control automated decision-making, please refer to question 7.1.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Obtaining consent and providing opt-out options are required when sending any commercial messages to individuals. Additional obligations may apply when the advertising activities involve automated decision making. To elaborate:

- (a) **Consent:** without prior consent or request from the customer, a company shall not send commercial messages. In practice, a bundled consent is generally enough, which means that if the customer consents to a privacy policy including clauses giving the company the right to send commercial messages, this can be deemed as consent for receiving commercial messages.
- (b) **Opt-out:** the company must offer convenient and effective ways for customers to decline to receive commercial messages, and inform customers of how to opt out. Common practices include providing an unsubscribe entry at the bottom of the email, or allowing the customer to reply with specified characters (eg 'TD') to unsubscribe. The company must also clearly state its name in the commercial message and indicate 'advertisement' or 'AD' in the title.
- (c) **Automated decision making:** if the information pushing or commercial marketing is based on automated decision making, the company should give customers options not specific to their personal characteristics or give them an easy way to refuse such communications. In practice, this usually appears as a 'close personalized recommendations' button in the app.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The use of vendors and other third parties in advertising typically involves sharing PI among different parties. In this respect, Chinese privacy law distinguish between different types of data cooperation models, ie, joint processing, entrusted processing, and providing PI to another PI processor.

Generally speaking, the use of vendors like DSPs and SSPs is categorized as entrusted processing, in which the vendors acts as an entrusted party, whose PI processing purpose and methods are determined by the PI processor (eg, advertiser). The PI processor should agree with the entrusted party on the purpose of processing, the time limit, the method of processing, the type of PI, the protection measures, and the rights and obligations of the two parties, and should supervise the entrusted party's PI processing activities. Records of such entrusted processing shall be kept for a minimum of three years. In addition, the PI processor must conduct a PI protection impact assessment.

The use of third-party data providers is generally categorized as 'providing PI to another PI processor'. In this regard, the advertisers should verify the legitimacy of the source of the data and the legitimacy of the basis for the data provider to provide the PI. A PI transfer agreement is also required for this kind of PI provision. The PI provider and recipient should agree on the purpose of processing, the time limit, the method of processing, the type of PI, the protection measures, and the rights and obligations of the two parties, and the PI provider should supervise the recipient's PI processing activities.

If the parties are engaged in joint processing (ie if they are both controllers and jointly decide on the purpose and method of the PI processing), they must agree on their respective rights and obligations.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Please refer to question 6.1.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Due diligence largely comes in the form of a PI protection impact assessment. This is required where a PI processor provides or entrusts the processing of PI to others. The impact assessment assesses whether the purpose, method or any other aspects of the processing of PI are lawful, legitimate and necessary; the impact on personal rights and interests and level of risk; and whether any security protection measures being taken are lawful, effective and commensurate with the level of risk. PI protection impact assessments are also required for sensitive PI processing, using PI for automated decision-making, public disclosure of PI, and PI exports.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Obtaining consent and providing opt-out options are required when sending any commercial messages to individuals. Additional obligations may apply when the advertising activities involve automated decision making. Please refer to question 5.3.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technology is not prohibited under Chinese law, but the information used and generated by many of these tracking technologies will be considered PI and thus be subject to PI regulations.

The 2020 Specification provides a template website privacy policy, which requires a website/app to disclose to its users how such website/app uses cookies and similar technologies for collecting PI, and how the user can restrict cookies or other similar technologies from collecting PI.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs, promotions, sweepstakes and other parallel market-building activities are regulated under advertising-related laws, but there are no specific privacy rules in this regard. If a program promoter collects or uses user PI, then it will have to comply with the general rules for the protection of PI.

7.4 How is social media and influencer marketing regulated under privacy law?

The PIPL and other privacy related laws will usually apply to social media in China. Large social media platforms have been a focus for various enforcement campaigns in this regard. In addition, most large social media platforms would likely reach the threshold amounts for PI processing that trigger stricter requirements. For example, large network platform service providers are required to publish an annual social responsibility report on personal information protection. Large social media platforms could also fall within the scope of a CIIO, which are subject to strict rules, including data localization.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted and behavioral advertising are allowed, but are becoming more heavily regulated, including at the national and local levels.

The PIPL requires that individuals should be given the right to opt out and demand an explanation (see question 5.2). These rights are elaborated and enhanced under the Administrative Provisions on Recommendation Algorithms in Internet Information Services ('Algorithms Provisions'), which are intended to introduce enhanced accountability and transparency into the operation of user-facing machine learning and algorithmic recommendation tools (see question 7.1).

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific privacy rules for digital identity resolution and clean room technologies. If a user of such technologies collects or uses PI, it will have to comply with the general rules.

7.7 How is location-based advertising regulated under privacy law?

Precise location data is classified as sensitive PI under Chinese privacy law. This generally refers to location information collected by calling the precise location permission of mobile phones. In contrast, rough location data estimated by IP address is not classified as sensitive PI.

PI processors may only process sensitive PI with separate (unbundled) consent, which includes notification to the PI subject of the need for such processing and the potential impact on the individual's rights and interests. In addition, the processing of sensitive PI must have a specified purpose, sufficient necessity for the processing, and strict protection measures, including that the PI processor must conduct a PI protection impact assessment.

7.8 How are data brokers defined and regulated under privacy law?

The DSL requires that institutions engaging in data transaction intermediary services must, when providing their services, require data providers to explain the source of the data, to examine and verify the identity of both parties to the transaction, and retain examination, verification, and transaction records.

7.9 How is advertising to children and minors regulated under privacy law?

PI of minors under the age of 14 is classified as sensitive PI. PI processors may only process such information when there is a specified purpose and sufficient necessity and there are strict measures adopted for its protection. In addition, processing the PI of minors under the age of 14 requires parental consent and specific PI processing rules. In parallel, there are obligations to block inappropriate content and implement anti-addiction mechanisms.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Profiling, the use of artificial intelligence and automated decision-making technology are allowed, but are becoming more heavily regulated:

- (a) **Transparency:** the PIPL requires that where a PI processor uses PI in automated decision-making, it must ensure the transparency of the decision-making. The Algorithms Provisions stipulate that recommendation algorithm-based service providers must inform users of their provision of recommendation algorithm-based services in a prominent manner and publicize the basic principles, purposes, and main operation mechanisms of the recommendation algorithm-based services in an appropriate manner.
- (b) **Fairness and impartiality:** Under the PIPL, this means no unreasonable differential treatment of individuals in terms of transaction prices or other transaction terms. The Algorithm-specific Governance Checklist Guidelines further stipulate that platforms must not have inconsistencies in the original pricing of the same goods for different users.
- (c) **Censorship/anti-addiction:** The Algorithms Provisions require that recommendation algorithm-based service providers strictly manage user models and tags, improve rules for including interest points in user models and user tags, and must not include prohibited information keywords in user interest points or use them as user tags to push information. It is also prohibited to set up algorithm models that lead users into addiction or excessive consumption, or use algorithm models that violate laws and regulations on ethics and morals.
- (d) **Individual rights:** the PIPL requires that if business marketing or push-based information delivery is conducted toward an individual by means of automated decision-making, an option for not targeting at the personal characteristics of the individual or an easy way to refuse to receive such information shall be provided to the individual. If a decision made by a personal information processor through automated decision-making has a material impact on an individual's rights and interests, the individual shall have the right to demand the personal information processor to provide an explanation, as well as the right to refuse the making of decisions by the personal information processor solely by means of automated decision-making. The Algorithms Provisions further requires recommendation algorithm-based service providers to provide users with the function of selecting or deleting user tags with respect to their personal characteristics to be used for recommendation algorithm-based services.

- (e) **Algorithm filing:** If the recommendation algorithm-based service is considered to have public opinion attributes or social mobilization capabilities, it will be subject to CAC filing procedures. The actual scope of ‘public opinion attributes or social mobilization capabilities’ is not yet clear, but in practice it is generally assumed that B2C recommendation algorithms may fall into this category. We note that some DSP platforms and media platforms have completed algorithm filing procedures in China.

7.11 Are there other specific advertising practices that you wish to discuss?

For digital advertising and marketing, techniques such as differential privacy and privacy computing are popular in China. However, there are questions around whether the data processed by adopting the above advanced technologies can truly achieve anonymization. If not, then the relevant data should still be regarded as PI and follow the rules for PI processing.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

- (a) Under the CSL, DSL and PIPL, entities seeking to transmit PI out of China are required to meet certain requirements, including:
 - (i) The PI subject must be notified of the name and contact information of the overseas recipient; the purpose and method of the processing; the type of PI involved; and how individuals can exercise their rights provided for by the PIPL against the overseas recipient;
 - (ii) The PI processor must obtain separate (ie, unbundled) consent from the PI subject (if consent is chosen as the grounds for PI cross-border transfer activities);
 - (iii) The PI processor must conduct a PI protection impact assessment.
 - (iv) The PI processor must take measure to ensure that the PI processing activities by overseas recipients meet the standards of personal information protection provided in the PIPL.
- (b) In addition, certain administrative procedures may be required depending on the cross-border data transfer scenario and the volume of PI to be transferred. These procedures, collectively referred to as ‘CBDT Procedures’, may include a CAC-led security assessment of the data transfer, implementation and filing of China standard contractual clauses (‘China SCCs’).
Data export activities falling into any of the below categories can be conducted without the need to complete CBDT Procedures:
 - (i) **Individual contractual necessity:** exporting PI that is necessary for the conclusion or performance of a contract to which the data subject is a party, such as cross-border shopping, delivery, remittance, payments, bank account opening, air ticket and hotel bookings, visa applications, examination services, etc.;
 - (ii) **Global HR management necessity:** exporting employee PI in accordance with enforceable employment policies and collective bargaining agreements for necessary cross-border human resources management;

- (iii) **Safety emergency necessity:** exporting PI for purposes of protecting individuals' life, health or property security in emergency situations; or
- (iv) **Low volume PI transfers:** non-critical information infrastructure operators (Non-CIIOs) transfer of PI (excluding sensitive PI) of less than 100,000 individuals from January 1 of the same year.

CAC-led security assessment applies to all cross-border PI or important data transfers by CIIOs, and where non-CIIOs transfer overseas the PI of more than 1,000,000 individuals (excluding sensitive PI) or the sensitive PI of more than 10,000 individuals, each on a cumulative basis starting from January 1 of the same year (the calculation should exclude the data under full exemptions).

SCCs filing and PI certification apply when non-CII operators transfer overseas the PI of more than 100,000 and less than 1,000,000 individuals (excluding sensitive PI) or the sensitive PI of less than 10,000 individuals on a cumulative basis starting from January 1 of the said year (the calculation should exclude the data under full exemptions).

- (c) There are no specific countries or jurisdictions where certain transfers are prohibited under Chinese privacy law. That said, when conducting CAC-led security assessment, SCCs filing and PI certification procedures, the PI protection policies, regulations, and network security environment in the country or region where the overseas recipient is located will all be factors under consideration.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The principles outlined above generally apply to all data transfers.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in China? Are there minimum standards? Does this differ by sector or size of the entity?

Data security and management requirements are scattered across several laws and non-binding standards. The top-level data-related laws provide general requirements, which may vary by entity size and sector (eg CIIOs have more obligations and restrictions). Industrial laws and regulations impose industry-specific security requirements. Various non-binding standards provide additional guidance:

The CSL, DSL, and PIPL stipulate the general data security obligations:

- (a) Under the CSL, network operators are responsible for taking technical and other necessary measures to ensure the security of the personal data they collect, establishing and improving their systems for user information protection, and preventing such information from being divulged, damaged or lost.
- (b) Under the DSL, data handling activities must comply with data security protection obligations, including: establishing and completing lifecycle data security management, taking corresponding technical and other necessary measures to ensure data security, and conducting relevant data security education and trainings.
- (c) Under the PIPL, PI processors must, based on the purpose and method of the processing, the type of PI processed, and the impact on personal rights and interests or any potential security risk, take the following measures to ensure the compliance of their PI processing with the law:

- (i) Prevent any unauthorized access to, leakage of, tampering with, or loss of the PI;
- (ii) Formulate an internal management system and operating procedures;
- (iii) Implement classified management system;
- (iv) Adopt corresponding technical security measures, such as encryption and de-identification; reasonably determine the operational authorization for PI processing;
- (v) Conduct security education and training for operational staff on a regular basis;
- (vi) Develop and organize the implementation of emergency plans for PI security incidents.

Additional data security obligations are imposed on CIIOs and large internet platforms.

9.2 How are personal data breaches regulated in China? What are the requirements for notification and response?

The handling of data breaches is regulated primarily under the PIPL as well as a few other laws. In general, the most fundamental requirement is that, in the event of data breach or data leakage, the PI processor and the Entrusted party must notify the authorities and affected individuals and take relevant remedial measures; failure to do so can result in civil, administrative, or criminal liabilities.

A PI processor is not obligated to notify the affected individuals if the PI processor can take measures to effectively avoid any harm that may be caused by the breach, but the authorities can insist on notification if they disagree with the PI processor's harm assessment.

Under the DSL, if a data processor discovers risks, such as data security flaws or vulnerabilities, it must immediately adopt remedial measures; and if a data security incident occurs, it must immediately take measures, notify users, and report the matter to the relevant authority. Additionally, anyone engaged in data handling activities 'using the internet or other information networks' must perform the same data security protection obligations listed above, but must do so with specific reference to the graded cybersecurity protection system.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Under the PIPL, failing to comply with requirements or obligations can result in significant penalties. These can range from rectifications and warnings to suspension of the relevant service, revocation of the entity's business license, or/and fines of up to RMB 50 million or 5% of global revenue. Executives in charge can also be fined and banned from holding certain corporate positions in future. In addition, the entity could be blacklisted from doing future cross-border transfers. In addition to administrative penalties, civil and criminal liability are possible in serious cases.

Under the DSL, any organization or individual failing to comply with the data security obligations when engaged in data processing activities can face significant penalties. These can range from rectifications, warnings, and fines of up to RMB 500,000 (approx USD 70,000). Executives in charge and other persons directly liable can also be fined up to RMB 100,000 (approx USD 14,000). Companies that refuse to rectify the conduct, or cause major data leaks or other serious consequences can be fined up to RMB 2 million (approx USD 280,000), and could concurrently be ordered to suspend the relevant business or cease operations for rectification, or have the entity's business license revoked; executives

in charge and other persons directly liable can be fined up to RMB 200,000 (approx USD 28,000). Any violations relating to 'Core Data' (ie data with relevance to the State) will face more serious penalties, including criminal liability. Under the CSL, for a 'severe' violation, a PI processor may face fines of up to RMB 1 million (approx USD 140,000) (or 10 x the illegal earnings), suspension of a related business, winding up for rectification, shutdown of any websites and revocation of a business license. The persons directly in charge may face a fine of up to RMB 100,000 (approx USD 14,000).

Data security breaches may also involve criminal liabilities. Under the Criminal Law, network service providers which do not fulfil legal obligations regarding information network security management provided in the laws and administrative regulations, and refuse to make rectifications after being ordered to do so by the relevant authorities (thus causing the leakage of users' information with serious consequences), may face a sentence of imprisonment or criminal detention of not more than three years, or surveillance and/or a fine.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, individuals can sue for civil compensation if their privacy rights or reputation are harmed. Such lawsuits would generally be brought under the Civil Code or the Law on the Protection of the Rights and Interest of Consumers, the CSL or the PIPL. There are several different possible causes of action under these laws. For example, in one case, an individual successfully sued an online travel service platform for big data-driven discriminatory pricing. Since the Civil Code came into effect on January 1, 2021, there have been numerous public interest lawsuits (similar to class actions) relating to privacy and data.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Administrative enforcements for cybersecurity, data security, and PI protection issues related to advertising have been more common in recent years, such as:

- (a) **Commercial marketing without prior-consent from the individuals.** For example, in 2013, a restaurant in Shanghai sent marketing calls and text messages to customers without prior consent. These actions were recognized as unlawful PI processing, and the restaurant was eventually sanctioned with a warning by the enforcement agency;
- (b) **Automated decision-making compliance:** For example, in a judicial case in Shanghai in 2022, a social platform app provided the function to opt-out of personalized advertising recommendations, but set a six-month validity period, after which the platform would automatically restore personalized advertising recommendations. The Shanghai Jinshan court held that it was lawful for the platform to provide advertising services and obtain revenue from such services, but it is prohibited for the platform to set an expiring validity period for opting-out of personalized advertising recommendations.
- (c) **App and mini-program PI collection and usage:** The CAC, MIIT and their local branches periodically conduct enforcement campaigns targeting the collection and use of PI by Apps and mini-programs, and publicize the investigation results. For the advertising industry, a key concern is PI collection and the use of third-party SDKs (eg, ads monitoring SDKs). For example, in 2024 the MIIT disclosed an ads SDK that lacked detailed disclosure of PI collection and use by the SDK and imposed a deadline for rectification.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in China?

Chinese data law particularly emphasizes data sovereignty. Data sovereignty is a key element in China's official discourse, emphasizing the Chinese government's authoritative control over data collection and the transmission of data across international borders. For example, the CSL and DSL gives the Chinese government extensive authority to access data held by companies operating within China, including the power to require technical support and assistance in matters of national security or criminal investigations.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

PI compliance audits, cross-border transfer, and with AI regulation are priority topics for both the public and the regulators in China right now:

- (a) **PI compliance audits:** The PIPL requires audits of PI processing activities to be conducted by PI processors. To refine these requirements, the CAC issued the Management Measures for Personal Information Protection Compliance Audits in February 2025. According to these Measures, PI processors processing the PI of more than 10 million people shall conduct PI protection compliance audits at least once every two years. The Measures also provide Guidelines for PI Protection Compliance Audits in the form of an annex. The future implementation of PI compliance audits should be monitored.
- (b) **Cross-border transfers:** China has tried to implement a relatively strict approach towards businesses engaged in cross-border data transfer. That said, based on the need to balance economic development and data security, the CAC released the Provisions on Facilitating and Regulating Cross-border Data Flows in March 2024, which significantly eased compliance burden, and built a new top-level framework for the deregulation of data exits (see question 8.1). Such optimization for cross-border data transfer activities is expected to continue. This may primarily be reflected at the local level, such as the continued release and adjustment of negative lists and exemptions in various FTZs.
- (c) **AI regulation:** With the development of AI, numerous personal privacy protection issues related to AI governance have emerged. To date, the Chinese government has released three major regulations addressing legal issues created by AI, ie, the Administrative Provisions on Recommendation Algorithms in Internet Information Services, the Administrative Provisions on Deep Synthesis in Internet-based Information Services, and the Interim Measures for the Management of Generative Artificial Intelligence Services. It is expected that more policy documents and standard frameworks would be released to provide more specific and practical technical guidance and behavioral norms for AI as the industry develops.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Data is seen as an important factor for production by the Chinese government, which has continuously advocated for the exploration and utilization of data assets as a new driver of economic growth. Aligning with this initiative, the central government established the National Data Bureau in 2023, and issued several policies aiming to strengthen data systems and unleash the market value of data elements. For example, in early 2024, the National Data Bureau and other departments jointly issued

the Three-Year Action Plan (2024-2026) for ‘Data Element ×’, calling for the development of data assets, while emphasizing the importance of maintaining data supply quality and ensuring data security. The practical impact of such initiatives remains to be seen.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

China’s privacy landscape has evolved rapidly since 2022, building on the foundational privacy laws established in 2021. Over the past years, the country has expanded regulations on personal information protection, data security, and cybersecurity, introducing stricter rules on cross-border data transfers, app data collection, and compliance certification.

A key shift has been the government’s effort to balance data security with technological innovation and economic growth. This is reflected in a more flexible and investor-friendly regulatory approach, particularly in cross-border data transfers, aimed at improving the business environment for private and foreign companies amid global economic and geopolitical shifts.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The major challenge for all companies handling data in China today is balancing the clearly increasing legal requirements against both the remaining uncertainty about exact implementation requirements in some cases, and the equally pressing need for companies to integrate their China data operations with their global information infrastructure. This means that companies need to be flexible and need to prioritize staying up to date on the continuously evolving requirements and expectations. In China’s fast moving privacy landscape, these rules can be difficult to navigate. Sometimes, ostensibly non-binding guidelines become de-facto requirements until final and binding laws are issued. Companies must be aware of this dynamic, as well as of any rules applicable to their specific sector, such as banking, the automobile industry, etc.

12.3 What do you envision the privacy landscape will look like in five years?

The next five years will see data compliance practice in China mature, as more detailed rules and precedential enforcement actions emerge. It is very difficult to anticipate exact outcomes, as the Chinese government is attempting to balance a continuing desire for domestic growth and foreign investment against a priority for information sovereignty and political stability. Nevertheless, we anticipate that we will see muscular regulation paired with more nuanced enforcement as a strong trend.

 COLOMBIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Colombia.

Privacy is regulated in Colombia based on the constitutional right of *habeas data*.

Habeas data is the right of citizens to know, update, rectify and delete information provided to third parties which has been incorporated into databases and public and private archives. Consequently, it is the entitlement of citizens to ensure that personal information granted to third parties and collected in databases or files is collected and treated properly.

1.2 What are the primary laws regulating privacy in Colombia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary regulation concerning privacy is Law 1581 of 2012 ('Data Protection Statute') by which general provisions for the protection of personal data are issued and its regulatory Decree 1377 of 2013, which facilitates its implementation and compliance.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Privacy law is not self-regulated in Colombia.

1.4 How is privacy law enforced in Colombia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy law can be enforced as follows:

- (a) **Direct claims:** A data subject or their successor who considers that the information contained in a database should be corrected, updated or deleted, or who notices an alleged breach of any of the duties of the Data Protection Statute, may file a complaint with the data controller or the data processor.

The maximum term to respond to the claim is 15 business days from the day following the date of receipt. When it is not possible to address the claim within this period, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed 8 business days.

- (b) **Claim before the SIC:** A data subject or their successor may only file a complaint with the competent authority, the Superintendence of Industry and Commerce ('SIC'), once proceedings of a direct claim before the data controller or data processor have been exhausted.

The SIC, once a breach of the provisions of the Data Protection Statute by the data controller or data processor has been established, will adopt the appropriate measures or impose sanctions.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Colombia?

All companies which perform the processing of personal data or own a database are subject to privacy law. In other words, the following persons/entities are subject to the privacy law in Colombia:

- (a) **Data Processor:** This is a natural (individual) or legal person (company), public or private, that by itself or in association with others, performs the processing of personal data on behalf of the data controller.
- (b) **Data Controller:** This is a natural (individual) or legal person, public or private, that by itself or in association with others, creates the database and/or the data processing.

2.2 Does privacy law in Colombia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Data Protection Statute applies to the processing of personal data:

- (a) carried out in the Colombian territory; or
- (b) when Colombian legislation is applicable to a data controller or data processor not established in national territory under international regulations and treaties.

Companies outside the country are not required to complete specific obligations, other than the ones established for companies located in Colombia. Thus, they are not required to have a representative in Colombia.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Colombia?

‘Personal data’ is defined as any information linked with, or that can be associated with, one or more determined or determinable natural persons (individuals).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive data’ is all information that may affect the privacy of the data subject or improper use of which may generate discrimination, such as data that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in syndicates, social organizations, of human rights or that promote interests of any political party or that guarantee the rights of opposition political parties as well as data related to health, sexual life and biometric data.

Processing of sensitive data is prohibited, except when:

- (a) the data subject has explicitly authorized the processing (except in cases where the granting of authorization is not required by law);
- (b) the processing is necessary to safeguard the vital interest of the data subject and the data subject is physically or legally incapacitated. In such cases, legal representatives must grant authorization;
- (c) the processing is carried out in the course of legitimate activities and with due guarantees from a foundation, NGO, association or any other non-profit organization, whose purpose is political, philosophical, religious or syndicate, provided that they relate exclusively to its

- members or to persons who have regular contact because of their purpose. In such cases, the data cannot be provided to third parties without the authorization of the data subject;
- (d) the processing relates to data necessary for the establishment, exercise or defend a right in a judicial proceeding; or
 - (e) the processing has a historical, statistical or scientific purpose. In this event, measures leading to the removal of identity of the data subjects must be adopted.

The processing must ensure respect for the rights of children and adolescents (The processing of the personal data of children and adolescents is prohibited, except for data that, due to its nature, is public). It is the task of the State and educational entities of all kinds to provide information and train legal representatives and tutors on the possible risks faced by children and adolescents regarding the improper treatment of their personal data, and instruct about the responsible and safe use by children and adolescents of their personal data, their right to privacy and protection of their personal information and that of others.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized, pseudonymized, or de-identified data treated are treated as security measures to protect personal data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The principles regarding the processing of personal information/personal data are:

- (a) **Legality:** The data processing referred to in the Data Protection Statute is a regulated activity that must be subject to the provisions of that statute and in the other provisions related to the subject;
- (b) **Purpose:** The data processing must be for a legitimate purpose in accordance with the Constitution and the Law, which must be communicated to the data subject;
- (c) **Freedom:** Data processing can only be carried out with the prior, express and informed consent of the data subject. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that relieves consent;
- (d) **Truthfulness or Quality:** The information subject to data processing must be truthful, complete, accurate, updated, verifiable and understandable. The processing of partial, incomplete, fractional or error-inducing data is prohibited;
- (e) **Transparency:** In data processing, the right of the data subject to obtain information about the existence of data concerning them must be guaranteed at any time and without restrictions from the data controller or the data processor;
- (f) **Access and restricted circulation:** The data processing is subject to the limits derived from the nature of the personal data, the provisions of the Data Protection Statute and the Constitution. Thus, processing may only be done by persons authorized by the data subject and/or by the persons authorized by law.

Personal data, except for public information, may not be available on the Internet or other means of disclosure or mass communication, unless access is technically controllable to provide restricted knowledge only to data subjects or authorized third parties in accordance with the Data Protection Statute;

- (h) **Security:** The information subject to data processing by the data controller or the data processor referred to in the Data Protection Statute should be handled with such technical, human and administrative measures as are necessary to grant security to the records, avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access; and
- (i) **Confidentiality:** All persons involved in the processing of personal data not categorized as public are obliged to guarantee the confidentiality of the information, even after the end of their relationship with any of the tasks included in the processing of data, and are only able to provide or communicate personal data when it corresponds to the development of the activities authorized in the Data Protection Statute and in the terms thereof.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

There are two main roles that may be assigned to a person/entity:

- (a) **Data controller:** this is the person/entity who is in charge of the collection of the information. The data controller is required to obtain authorization from the data subject concerning the processing of the personal data.
- (b) **Data processor:** The processing of the personal data can be delegated to a data processor. The principal responsibility of the data processor is the due management of the database.

4.3 **Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

Yes, the processing of personal data requires prior, express and informed consent from the data subject, except in cases where the granting of authorization is not required by law.

5 **TRANSPARENCY AND CONSUMER RIGHTS**

5.1 **What information must companies include in their privacy notices when processing personal data for advertising purposes?**

The data controller, at the time of requesting the data subject's authorization, must clearly and expressly inform them of the following:

- (a) the processing to which their personal data will be subjected and the purpose thereof;
- (b) that responding to questions is voluntary, when such questions pertain to sensitive data or data concerning children and adolescents;
- (c) the rights to which they are entitled as a data subject;
- (d) the identification, physical or electronic address, and telephone number of the data controller.

5.2 **What privacy rights do consumers have concerning their personal data in advertising contexts?**

A data subject who is an individual has the following rights:

- (a) to know, update and rectify the personal data with the data controller and/or the data processor. This right may be exercised, inter alia, against partial, inaccurate, incomplete, fractional, or error-inducing data, or data whose processing is expressly prohibited or has not been authorized;

- (b) to request proof of the authorization granted to the data controller (except in cases where authorization is expressly excepted as a requirement for the data processing, in accordance with the provisions of the Data Protection Statute);
- (c) to be informed by the data controller and/or the data processor, upon request, regarding the use given to the data subject's personal data;
- (d) to submit complaints to the SIC regarding violations of the provisions of the Data Protection Statute and other related regulations;
- (e) to revoke authorization and/or request the deletion of data when the constitutional and legal principles, rights and guarantees are not respected in the processing. The revocation and/or deletion will proceed when the SIC has determined that, in the data processing, the data controller and/or the data processor have engaged in conduct contrary to the Data Protection Statute and/or the Constitution; and
- (f) to access, free of charge, their personal data that has been subject to processing.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

In the processing of personal data, the prior and informed authorization of the data subject is required, which must be obtained through means that allow for subsequent consultation.

Additionally, consumers may revoke their authorization and/or request the deletion of their data when there is no legal or contractual obligation requiring its retention in the referenced database.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

This is governed by the general principles. Thus, advertising agencies, DSPs, SSPs, or data providers and others must obtain prior, express and informed authorization from data subjects for the processing of personal data.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies must verify that the authorization they have obtained from data subjects includes the possibility to disclose personal data to third parties and the purpose of said disclosure.

Companies can not disclose nor receive personal data from data subjects who have not authorized the transference of their data or when the purpose of the authorization does not extend to disclosing or receiving personal data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must:

- (a) eliminate all personal data relating to data subjects when no authorization has been issued from that data subject;
- (b) only process personal data when an authorization has been obtained prior to any data processing;

- (c) have the following manuals:
 - (i) security policy,
 - (ii) processing of private data policy, and
 - (iii) due attendance of questions and claims.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The only contact information which can be used to send marketing communications is that which the data subject has explicitly authorized for such use. Thus, the use of personal data for marketing must be previously authorized in accordance with the provisions of the Data Protection Statute.

In cases where an individual receives a marketing communication which has not been authorized, the recipient may initiate proceedings against the advertiser.

This has been considered in several decisions from the SIC, from which it is clear that the gathering of contact information must be authorized in advance (or, at the latest, at the moment of collection) and that the use for which the information is being collected should be clear and sufficient, so that the data subject can control the use of their information.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

This is governed by the general principles.

The essence of *habeas data* is integrated with the right to data self-determination and freedom. Data self-determination is the power of the data subject to authorize their personal data's conservation, use and circulation, in accordance with legal regulations. Thus, without the consent of the data subject, this fundamental right is violated, as it unjustifiably restricts the data subject's self-determination regarding their personal information, since the administration of their data, regarding the collection, treatment and disclosure, would be done without authorization.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs are authorization-based. Thus, programs can only use information for the purposes expressly permitted by the data subject.

7.4 How is social media and influencer marketing regulated under privacy law?

- (a) **Social networks:** These cannot collect or treat personal information without free, prior and express consent from the data subject.
- (b) **Third parties:** A data controller may only contact a data subject through the mechanisms previously and expressly authorized by the data subject, and such consent cannot be extended to the linking of this information through the use of mobile instant messaging applications or social networks.
Thus, for a third party to contact the data subject through instant messaging or social media applications, it must in every case obtain prior, clear and express authorization for this purpose.

- (c) **Users:** Users of social media are governed by Article 15 of the Constitution, by which all individuals are entitled to their fundamental right of privacy. Hence, users cannot post or disclose information that may affect the privacy of others or affect their image or good standing.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising is not specifically regulated. Thus, its regulation is based upon the general rules. As per the principles ruling privacy, there is a ban on creating a profile based on data analysis. This translates into a proscription on being subjected to adverse legal effects due to an evaluation of one's personality through an automated treatment of data intended to evaluate certain aspects of personality, or in connection with data that is considered as sensitive.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not specifically regulated. Thus, their regulation is based upon the general rules. See question 7.5.

7.7 How is location-based advertising regulated under privacy law?

Location-based not specifically regulated. Thus, their regulation is based upon the general rules.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are not specifically regulated. Thus, regulation is based upon the general rules.

Information operators may provide personal information verbally or in writing collected or provided in accordance with the provisions of the Data Protection Statute, to the following persons:

- (a) the data subject,
- (b) persons duly authorized by the data subject;
- (c) the successors of the data subject;
- (d) the users of information;
- (e) the judicial authority after a court order;
- (f) the public entities of the executive branch in the exercise of their functions;
- (g) the supervisory bodies and other entities of disciplinary, fiscal, or administrative investigation;
- (h) other data operators when authorization is obtained from the data subject or when the authorization of the data subject is not required by the destination data bank, as it has the same purpose or purpose as that of the operator who delivers the data; and
- (i) the persons authorized by the Data Protection Statute.

The contact information and personal data can only be registered and disclosed with the free, prior and express consent from the data subject, as per the Data Protection Statute.

7.9 How is advertising to children and minors regulated under privacy law?

In the processing of personal data, respect for the rights of children and adolescents must be ensured. The processing of personal data of children and adolescents is prohibited, except for data of a public nature.

The processing of personal data of minors is only permitted when the following criteria are met:

- (a) the purpose of the processing serves the best interests of children and adolescents;
- (b) respect for their fundamental rights is ensured;
- (c) the opinion of the child or adolescent is considered according to their level of maturity; and
- (d) the principles established in the Personal Data Protection Statute for the processing of personal data are complied with.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Profiling is not specifically regulated. Thus, their regulation is based upon the general rules. As per the principles ruling privacy, there is a ban on creating a profile based on data analysis. See question 7.5.

7.11 Are there other specific advertising practices that you wish to discuss?

Colombia is not used to regulate particular uses, or specific purposes. Instead, the law has a general scope that applies to most situations which allows for the technology and the situations to change and still be applicable in all cases.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The transfer of personal data of any kind to countries that do not provide adequate levels of data protection is prohibited. It is understood that a country offers an adequate level of data protection when it meets the standards set by the SIC on the subject, which in no case may be lower than those required in Colombia.

This prohibition does not apply:

- (a) where the data subject has granted express and unequivocal authorization for the transfer of the information;
- (b) to the exchange of medical data, when required by the data subject's medical treatment for reasons of health or public hygiene;
- (c) to bank or stock transfers, in accordance with the applicable legislation;
- (d) to transfers agreed in the framework of international treaties to which Colombia is a party, based on the principle of reciprocity;
- (e) to transfers necessary for the execution of a contract between the data subject and the data controller, or for the execution of pre-contractual measures, provided that the data subject has authorized this; or
- (f) where legally required in order to safeguard the public interest, or for the recognition, exercise or defense of a right in a judicial process.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Companies interested in international data transfer are required to obtain a declaration of conformity from the SIC.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Colombia? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is governed by the principles of access and restricted circulation and security.

Thus, personal data, other than public information, may not be available on the Internet or other means of disclosure or mass communication, unless access is technically controllable to provide restricted knowledge only to data subjects or authorized third parties in accordance with the Data Protection Statute.

Furthermore, personal data should be handled with the technical, human and administrative measures that are necessary to grant security to the records, avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access.

Consequently, the data controller or the data processor must adopt measures to preserve the information and implement security controls that minimize the risk of data leakage or adulteration.

Finally, the data controller must keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.

9.2 How are personal data breaches regulated in Colombia? What are the requirements for notification and response?

The data controller must inform the SIC when there are violations of the security codes and there are risks in the administration of the information of the data subjects.

Thus, when a security breach occurs entailing risks for the personal data included in the database, the data controller and/or the data processor must inform the SIC, as data protection authority, that a data breach has occurred.

Consequently, a brief must be filed before the SIC, explaining:

- (a) the protective measures under which the database was safeguarded (eg, in a case against a bank in Colombia, the SIC pointed out that the bank had failed to demonstrate that it had implemented security measures to avoid the exposure of personal data of the data subjects);
- (b) how and when the data breach occurred; and
- (c) all the measures taken to undermine the breach and its effects (eg, in the same case against the bank, the SIC found that the bank had failed to prove security protocols to limit or minimize the risks for the processing of personal data).

It is also important to determine the number of data subjects affected by the breach.

Lack of notification is taken as a contributing factor that will enhance the sanction in cases where an investigation is initiated. On the other hand, notification is a mitigating factor. Article 24(f) of the Data Protection Statute states: ‘The penalties for infractions ... will be graduated according to the following criteria: ... The express acknowledgment or acceptance made by the investigated party about the commission of the infraction before the imposition of the sanction that may arise.’

To benefit from the mitigating factor, the data controller and/or the data processor could simply notify the breach or accept the breach within the course of an investigation. However, a better scenario would be for an acknowledgment (notification), as it allows them to explain to the authority the extent of the

damage and the economic benefit obtained by the infringer or third parties, by virtue of the commission of the infraction; which are other two factors taken into account to graduate the penalty. For example, in a case against a university concerning a security breach, the penalty was reduced from 40 to 30 times the monthly legal minimum wage (approx US \$8,280), since the university accepted that it had suffered a security breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The SIC may impose the following sanctions on the data controller and/or the data processor:

- (a) fines of a personal (individual) and institutional nature up to the equivalent of 2,000 times the legal monthly minimum wage in force at the time of the imposition of the sanction (approx USD 700,000). Fines may be successive as long as the breach that originated them persists;
- (b) suspension of the activities related to the data processing for a term of 6 months;
- (c) where the term of suspension has elapsed without the adoption of the corrective measures ordered by the SIC, temporary closure of operations related to the processing may be imposed; and
- (d) immediate and definitive closure of an operation that involves the processing of sensitive data.

10.2 Do consumers have a private right of action? What remedies are available to them?

Individuals have a private right of action; however, the proceeding does not contemplate compensation for damages for the data subject and remedies are therefore the same as those listed in question 10.1, ie, fines, suspension or closure.

If there is damage that should be compensated, the individual should initiate a declarative civil proceeding.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Very active. There is a famous case with advertisement in Facebook, involving the image of a child, which was decided by means of Resolution 69225 of 2023.

The facts of the case were that LIMONAR CONSTRUCTORA SAS provided a photograph of a minor to Transforma Publicidad SAS for the creation of an advertising piece on Facebook. The minor's mother later discovered the photograph on social media. At no point was authorization granted for the taking or publication of the photographs. As the photographs of the minor were taken by a photographer who provides images for advertising purposes, none of the criteria by which processing of a minor's personal data is permitted applied (see question 7.9). Therefore, the company in question was required to obtain the prior, express, and informed authorization of the minor's legal representative and to verify that the photographer had also obtained such authorization.

Pixelating the image does not eliminate the obligation to obtain authorization.

Consent is an essential element in the management of personal data, and it must be duly qualified, meaning it must be prior, express, and informed.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Colombia?

There are no rules particular to the culture of Colombia which affect privacy.

However, the Constitutional Court may consider cases related to privacy, as this is a fundamental right, and may issue guidelines not previously contemplated by the competent authority.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

There are still some topics to be regulated, especially regarding new technologies. However, currently there are no pending hot topics or laws on the way.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The main caution in Colombia is the importance of safeguarding the authorization granted by the data subject, as proof of the data subject’s consent may be required by the competent authority.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The main change that has occurred is in the number of advertising messages and the timeframes during which individuals may be contacted for debt collections or with commercial information. The change was triggered due to the amount of commercial calls received by individuals and the times at which those calls were made.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The main issue is that the system applies not only to a company’s executives but also to each of its employees, requiring each individual to assume the privacy system as a personal responsibility.

12.3 What do you envision the privacy landscape will look like in five years?

- (a) Recognition of data subjects and the value of the data they provide.
- (b) Payment to individuals for the provision of private data.

 COSTA RICA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Costa Rica.

Data protection in Costa Rica is regulated by Law No 8968 on the Protection of Persons Regarding the Processing of their Personal Data ('Data Protection Law') and Executive Decree No 37554-JP ('Data Protection Regulation'). However, the right to data protection has been recognized and protected in Costa Rica by the Constitutional Court since the 1990s, on the basis of Article 24 of the Political Constitution of Costa Rica, which specifically recognizes the right to intimacy, as well as the freedom and secrecy of communications.

1.2 What are the primary laws regulating privacy in Costa Rica? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The following are the key laws regulating privacy in Costa Rica:

- (a) Data Protection Law;
- (b) Data Protection Regulation; and
- (c) The chapter concerning electronic commerce of Decree No 37899-MEIC ('Consumer Protection Regulation').

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There is no any significant self-regulation in privacy regulation in Costa Rica.

1.4 How is privacy law enforced in Costa Rica? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The regulator in Costa Rica is PRODHAB. However, the National Consumer's Commission also has jurisdiction when consumer protection issues are involved (mainly in the context of e-commerce transactions). There are no self-regulatory bodies dealing with privacy.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Costa Rica?

Any company (private or public) that processes personal data of individuals residing in Costa Rica is subject to the privacy laws. This, irrespective of whether the database is automated or manual, and regardless of its location.

2.2 Does privacy law in Costa Rica apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Data Protection Law applies to any individual or entity that stores or uses the data of a Costa Rican resident. It is also applicable if so stipulated in a contract or mandated by any rule of international law. All actions taken by such individuals or entities will be subject to Costa Rican laws. While foreign-based entities are not generally required to appoint a local representative, they must do so if the database requires registration. In such cases, designating a representative is mandatory for both domestic and international entities.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Costa Rica?

The Data Protection Law defines ‘personal data’ as any information that relates to an identified or identifiable living individual.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Data Protection Law establishes the following categories of personal data:

- (a) **Unrestricted access personal data:** data contained in public and open databases with general access, the use of which is governed by specific laws and pursuant to the purpose for which such data were collected;
- (b) **Restricted access personal data:** data that may be accessed and stored only with authorization; and
- (c) **Sensitive personal data:** information concerning the intimate realm of the person, that may not be stored except in very specific circumstances. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, spiritual convictions, socio-economic condition, biomedical or genetic information, health, sexual life and orientation.

Sensitive Data can only be processed where processing:

- (i) is necessary to protect the vital interests of the data subject, or in other circumstances where the data subject is physically or legally incapable of giving consent;
- (ii) is undertaken by a foundation, association, or other body for political, philosophical, religious or union purposes, provided that the personal data is that of its members or regular contacts and the processing is undertaken in the course of its legitimate activities and in accordance with the law, and provided that the consent of the data subject is obtained for transfers to third parties;
- (iii) relates to sensitive personal data that the data subject has voluntarily made public, or is required for the recognition, exercise or defense of a right in judicial proceedings; or
- (iv) is necessary for medical or health purposes, provided that the processing is undertaken by a person in the medical profession, subject to professional secrecy obligations or the equivalent.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

There is no formal definition for these concepts.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The Costa Rican Data Protection Law requires that all information that it is handled must be up-to-date, truthful and adequate to the purpose that was requested. Also, it is mandatory to ensure that every person included in any database will have the right to access, rectify, revoke or cancel their authorization to store and use their personal information.

Finally, from a consumer protection perspective, all the information must be provided in Spanish.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

There are no relevant provisions for agreements between data controllers and data processors. The only aspect related to this matter is provided in the Data Protection Regulation, which states that the data processor should process the personal data in accordance with the agreement made with the data controller.

The Data Protection Regulation imposes some obligations on data processors and, in general, requires that the data processor guarantees the integrity and security of the information. In particular, the data processor must:

- (a) process personal data following the data controller's instructions;
- (b) refrain from processing personal data for purposes other than those instructed by the data controller;
- (c) implement security measures and comply with any minimum performance protocols;
- (d) maintain the confidentiality of the data that has been processed;
- (e) avoid proceeding with a data transfer unless duly instructed to do so by the data controller; and
- (f) delete personal data as soon as the relationship with the data controller has ended.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, an informed consent is necessary for processing personal data. No other basis for processing is included in the law.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

There is no formal list of required information. However, companies must comply with applicable laws and regulations, and these notices are typically used to ensure compliance.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) **Right to informed consent:** Data subjects have the right, when requested to provide their personal information, to an informed consent (see question 4.3). Express consent is not needed in the case of a few exceptions, namely:
 - (i) there is a reasoned order issued by a competent judicial authority, or an agreement adopted by a special investigative committee of the Legislative Assembly in the exercise of its office;
 - (ii) it is personal data of unrestricted access, obtained from sources of general public access; or
 - (iii) the data must be provided as a result of a constitutional or legal provision.

In addition, the main rights of each data subject are:

- (b) **Right of access:** Is the right of data subjects to receive, free of charge, within five working days after submitting a request, information from the data controller as to whether any of their data is held, an accurate report of the information on them being processed, and even extensive information, in writing (whether digitally or physically) concerning all the data being processed, as long as this does not affect third party rights;
- (c) **Right of rectification:** Data subjects are entitled to request the modification of all incomplete, inaccurate, and/or unclear data; and
- (d) **Right to deletion:** Data subjects may request, at any time, the deletion of their personal information. The data controller may refuse such a request only under the following circumstances:
 - (i) the data should be maintained in order to comply with other laws;
 - (ii) the data is needed for security reasons;
 - (iii) the data is needed in order to prevent and/or investigate any crime;
 - (iv) the data is needed to provide a public service;
 - (v) the data is unrestricted personal data; or
 - (vi) the personal data was anonymized.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Opt-out options are not permitted.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The Data Protection Regulation includes some obligations for data processors and, in general, requires that the data processor guarantees the integrity and security of the information. As to the obligations imposed on data processors, see question 4.2.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

There are no formal requirements for such agreements.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Impact assessments are not required in Costa Rica.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Initially, marketing communications were regulated in the Telecommunications Law, which covered only direct sales. However, subsequent regulations have extended regulation to cover other forms of commercial communications, such as promotional marketing and/or advertising in general.

Any marketing communication made through email must:

- (a) clearly identify the sender;
- (b) be done simply enough to easily identify the purpose of the message; and
- (c) include a valid email address to which the recipient of the message may send a request to suspend any further message, at no cost to the recipient.

The following forms of conduct are expressly mentioned in the regulations as unfair and/or fraudulent:

- (i) **Unsolicited advertising ('adware')**: ie information sent through the web to users related to the sale of a product or a service without the consent of the recipient;
- (ii) **Unsolicited communications**: ie any sort of communication generated by automated call systems, fax, email, call centers, person to person, SMS, etc, with the purposes of selling or soliciting sales of a product or service without the prior consent of the recipient;
- (iii) **Unauthorized operation of, access to and monitoring a terminal**: ie inserting an apparently harmless code into a computer to establish a 'backdoor' that allows the manipulation of the affected computer, compromising the confidentiality, functionality and the information stored in that computer;
- (iv) **Spreading viruses**: ie sending mass emails or other messages with the purpose or the consequence of contaminating the recipient terminal with a virus; and
- (v) **Unsolicited mass emails (SPAM)**: ie emails of unknown senders within the web, who constantly change their domains or usernames with the purpose of defeating the filters against unwanted messages.

Nevertheless, there is not strong enforcement against these practices.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There is no specific regulation for using tracking technologies.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs are not specifically regulated by data protection laws. They are subject to the general rules.

7.4 How is social media and influencer marketing regulated under privacy law?

There is no specific law regulating influencer marketing. However Law No 7472 on Consumer Protection and the Consumer Protection Regulation include some specifications that are applicable to influencers in some cases. These obligations include, among others, that influencers must clearly indicate that a payment has been received (ie, by including #ad). Thus, it must be made clear beyond any doubt that the publication results from having received some type of benefit (whether in cash or in kind) and is not an impartial and spontaneous opinion of the influencer.

It is important to highlight that non-compliance with this obligation can be considered, according to the mentioned Law, as misleading advertising since it would present a favorable image of a service without indicating that a benefit was received for such a comment. This can lead to consequences for both the influencer and the advertiser, including fines of up to 40 times the base salary, and could even result in lawsuits from a competitor.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

This is not regulated in Costa Rica.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

This is not regulated under privacy law.

7.7 How is location-based advertising regulated under privacy law?

This is not regulated under privacy law.

7.8 How are data brokers defined and regulated under privacy law?

No, there is no specific regulation for data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

The Law does not establish any particular regulation regarding the personal data of children. In Costa Rica, the age of majority is 18. Thus, anyone below 18 is considered a minor.

Moreover, any action taken by someone under 15 will be null and void; therefore any consent that a minor under 15 years of age may give will not be valid and their information cannot be collected without express consent from their parent or guardian.

If the minor is between 15 and 18 years of age, all contracts, agreements and any other economic activity (ie, online activity) are presumed valid, but may be annulled if one of the representatives of the minor requests its annulment. Therefore, it is possible to collect information from individuals between 15 and 18 years of age without any inconvenience, but this will be on the basis that they (or their parents) are able to revoke consent at any time without any inconveniences or consequences.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Neither artificial intelligence nor automated decision-making technologies are regulated in Costa Rica.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The Data Protection Law requires that data controllers obtain consent from the data subject in order to transfer personal data to another country. Note that it does not include special regulations for specific countries. Rather, all countries have the same requirements.

The transferor must ensure that, where information is transferred to any other country, adequate levels of protection of data subjects' rights in connection with the processing of their personal data will be provided.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Costa Rica? Are there minimum standards? Does this differ by sector or size of the entity?

The Data Protection Law provides that the data controller must conduct all technical and organizational safeguards in order to avoid the loss, destruction, alteration and/or unauthorized access of personal data. There are no specific minimum requirements nor standards.

9.2 How are personal data breaches regulated in Costa Rica? What are the requirements for notification and response?

In the event of a data breach, a data breach notification is mandatory. The requirements relating to data breach notifications are that:

- (a) The data controller must notify the data subjects and the PRODHAB within five business days following the discovery of the breach;
- (b) Within that same period (ie, five business days), the data controller must initiate a thorough review to determine the extent of the damages caused by the breach, and the corrective and preventive measures that must be adopted; and
- (c) The notification to affected data subjects and PRODHAB must include, as a minimum, the following information:
 - (i) the nature of the incident;
 - (ii) the compromised data;
 - (iii) the corrective measures taken immediately upon notice of the breach; and
 - (iv) contact information and place where more details about this matter can be obtained.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The competent authority in charge of imposing sanctions for non-compliance with the Data Protection Law is PRODHAB. In some specific circumstances, other authorities may be involved. For example, if a violation of a fundamental right is at issue, the case would be decided by the Constitutional Court, or, in the context of an e-commerce transaction, the National Consumer's Commission may also impose penalties.

PRODHAB may initiate proceedings *sua sponte*, or upon request by a person with a legitimate interest or subjective right. After receiving such a request, PRODHAB will grant database administrators three working days to reply and offer evidence considered relevant for their defense. PRODHAB can also investigate and gather evidence, and may issue any interim and provisional measures that it deems necessary. Proceedings end with a final judgment which is subject to appeals.

For an offense under the Data Protection Law, PRODHAB can issue sanctions which can be minor, serious or extremely serious. The penalty will vary depending on the seriousness of the offense, with fines ranging from approximately USD 3,000 to USD 18,000.

10.2 Do consumers have a private right of action? What remedies are available to them?

Individuals may file a claim at PRODHAB. Where the claim is well founded, the agency may order to the data controller to proceed with the request of the individual and/or impose a fine.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement actions in Costa Rica are very rare.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Costa Rica?

Actions to enforce privacy laws in Costa Rica are very rare. Consumers are not used to filing claims against entities using their personal data for marketing purposes.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

There is an important modification of the Data Protection Law that is being discussed at Congress at the moment.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

N/A

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

There isn't a changing privacy landscape at this point in Costa Rica.

12.3 What do you envision the privacy landscape will look like in five years?

A modification of the Data Protection Law is likely to happen within the next five years, increasing PRODHAB's enforcement powers and the obligations imposed on companies. However, it is difficult to estimate when this modification will happen.

 CURAÇÃO 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Curaçao.

Privacy is regulated in the National Ordinance for the Protection of Personal Data (Official Gazette 2010 no 84) ('Privacy Ordinance').

1.2 What are the primary laws regulating privacy in Curaçao? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy law is based on the Privacy Ordinance.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There is no self-regulation.

1.4 How is privacy law enforced in Curaçao? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Commission for Protection of Personal Data is in charge of supervising compliance with the Privacy Ordinance and administrative enforcement. Infringers can also be prosecuted via civil and criminal actions.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Curaçao?

A company is subject to privacy law in Curaçao if it is a legal entity established in Curaçao that processes personal data in connection with activities in Curaçao.

Exceptions are made for where personal data is processed:

- (a) by, or on behalf of, intelligence and security services;
- (b) for the performance of police tasks;
- (c) for the implementation of the National Ordinance Basic Administration of Personal Data;
- (d) for the implementation of the National Ordinance Judicial Documentation; and
- (e) on the statements regarding the conduct and for the implementation of the Election Regulation.

Another exception is if personal data is processed for journalistic, artistic or literary purposes; however, processing must be done properly and carefully, for an explicitly defined and justified purpose, and must comply with certain conditions under the Privacy Ordinance.

2.2 Does privacy law in Curaçao apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Privacy law applies to foreign companies if they are using automated or non-automated means located in Curaçao, unless these means are only used for the transfer of personal data. Foreign companies may only process personal data if a resident representative is appointed.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Curaçao?

Personal data is any information concerning an identified or identifiable natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Privacy Ordinance maintains the term ‘exceptional personal data’ for sensitive data, which is a person’s religion or belief, race, political affiliation, health, sexual life, as well as personal data regarding membership of a trade union, criminal personal data and personal data about unlawful or nuisance behavior in connection with a prohibition imposed as a result of that behavior.

Processing of exceptional personal data is prohibited, but there are certain exceptions:

- (a) Personal data pertaining to religion or belief may only be processed by churches or communities on a spiritual basis or by other institutions on a religious or philosophical basis;
- (b) Personal data pertaining to race may only be processed for identification purposes, if unavoidable for such purposes, or—under certain conditions—in the scope of preferential policy to lift or minimize actual disadvantages;
- (c) Personal data pertaining to political affiliation may only be processed by institutions based on political grounds regarding their members or employees or affiliated persons in connection with its goal or in mind of reasonable requirements to fulfil functions in administrative or advisory bodies;
- (d) Personal data pertaining to membership of trade unions may only be processed by the relevant trade union or trade union federation to which the trade union belongs insofar such is necessary to realize the goal of the trade union;
- (e) Personal data pertaining to health may only be processed for certain purposes by certain categories of controllers, such as healthcare providers, healthcare or social services institutions, insurance companies, special schools, probation institutions, guardianship council, administrative bodies and executive institutions that implement certain social security laws; and
- (f) Personal data pertaining to criminal personal data may in principle only be processed by a limited group of controllers under certain conditions.

In all of the abovementioned cases, the applicable rules for processing personal data must be observed at all times.

Nonetheless, personal data may be processed if:

- the individual has consented explicitly in writing to processing personal data or has made the data publicly available themselves, or
- processing is necessary to determine, exercise or defend a right in legal proceedings or to comply with an obligation under international law, or is necessary in light of a weighty general interest where there appropriate safeguards are offered or an exemption has been granted.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

There is no specific provision for anonymized, pseudonymized, or de-identified data.

However, the Privacy Ordinance applies if there is a real possibility that anonymized, pseudonymized, or de-identified data can be traced to an individual. It is recommended to take appropriate measures to minimize the risks for the individuals involved.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Personal data must be collected for specific, explicitly described and legitimate purposes.
- (b) It must be processed in a proper and careful manner and not further processed in a way that is incompatible with the purposes for which it was obtained.
- (c) Personal data must be adequate, relevant and not excessive considering its purpose and must be correctly and accurately reflected.
- (d) Confidentiality must be observed for personal data.
- (e) Personal data must not be stored longer than is necessary for the purpose for which it is processed.
- (f) There must be appropriate technical and organizational measures to secure personal data against loss or wrongful processing. Such measures must guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, in view of the risks involved in processing and the nature of the personal data to be protected. The measures must also prevent unnecessary data collection and further processing of personal data.

The Privacy Ordinance does not contain specific requirements relating to training, but companies are advised to inform and train their staff members on their obligations under the law, including secure handling of personal data and the rights of individuals.

If companies engage third-party data processors, they are required to have a written contract in place outlining the data processor's obligations, including the security measures in place, the purpose of processing, and ensuring that the data processor complies with the instructions of the controller.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, there are the roles of controller (responsible party) and processor:

- (a) The **controller** bears primary statutory responsibility for complying with the Privacy Ordinance.
The controller determines the purpose and resources for processing personal data and ensures that the processor takes sufficient technical and organizational security measures to protect personal data and prevent unnecessary data collection and further processing of the data and supervises compliance by the processor with such measures. In addition, the controller ensures that the processor processes personal data further to its instructions.

- (b) The **processor** processes personal data to the benefit and further to the instruction of the controller, but is an independent party.
Processing of personal data by processors is governed by an agreement or by virtue of another legal act that creates a commitment between the processor and the controller.
If the processor is not established in Curaçao, the controller must ensure that the processor complies with the law of that other country.

For evidence purposes, the parts of the agreement or legal act relating to the protection of personal data, as well as the security measures to protect personal data, must be laid down in writing or in another equivalent form.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes. Personal data may only be processed in the following cases:

- (a) the individual has given clear consent for data processing;
- (b) data processing is necessary to implement an agreement to which the individual is party, or to take pre-contractual measures that are necessary for concluding an agreement further to the individual's request;
- (c) data processing is necessary to comply with a legal obligation to which the controller is subject;
- (d) data processing is necessary to safeguard the vital interests of the individual;
- (e) data processing is necessary for the proper performance of a public-law task by the relevant administrative body or the administrative body to which the data is provided, or
- (f) data processing is necessary to protect the legitimate interest of the controller or of a third party to whom the data is provided, unless the interest or the fundamental rights and freedoms of the data subject, in particular the right to privacy, prevails.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

It is advised to include at least the following information:

- (a) the name and contact details of the company;
- (b) the purposes of data processing;
- (c) the lawful basis for processing;
- (d) the rights of data subjects;
- (e) the type of personal data being processed;
- (f) information about third-party recipients of the personal data;
- (g) the retention period of the personal data;
- (h) use of cookies and tracking technologies; and
- (i) whether profiling is to be carried out

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have a right to:

- (a) be informed if their personal data is being processed;
- (b) be informed about the details concerning processing of their personal data (eg, type of data, purpose, identity of controller, and other information in view of the nature of the personal data, the circumstances under which such was obtained or the use that is made thereof to guarantee to the individual that personal data is appropriately and carefully processed); and
- (c) request that their personal data be modified, protected or deleted.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Consent is particularly required for direct marketing (opt-in option). Opt-out options must be provided to object to direct marketing communications (eg unsubscribe links in emails).

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

There is no specific provision for this in the Privacy Ordinance, but it can be said in general that advertisers must take appropriate privacy and data protection measures for handling personal data and impose such measures on vendors and other third parties. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

There is no specific provision for this in the Privacy Ordinance. Companies must observe the general principles of processing personal data when disclosing or receiving such data to or from vendors and observe the rights of the individual, as well as generally accepted international standard practice.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must observe the general principles of processing personal data as well as generally accepted international standard practice in such cases. The Privacy Ordinance does not regulate impact assessments, though these may be recommendable when pertaining to activities involving sensitive personal data.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

There are no specific stipulations for marketing communications. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There are no specific stipulations for tracking technologies. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific stipulations for loyalty programs and promotions. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.4 How is social media and influencer marketing regulated under privacy law?

There are no specific stipulations for social media. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are no specific stipulations for targeted advertising and behavioral advertising. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific stipulations for identity resolution and clean room technologies. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.7 How is location-based advertising regulated under privacy law?

There are no specific stipulations for location-based advertising. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific stipulations for data brokers. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.9 How is advertising to children and minors regulated under privacy law?

There are no specific stipulations for advertising to children and minors. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific stipulations for profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes. The general principles of processing personal data apply, and the rights of the individual must be observed, as well as generally accepted international standard practice.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There are no requirements or restrictions concerning data transfer to a country that belongs to the Kingdom of the Netherlands (ie, Aruba, St Maarten, the Netherlands, and the Caribbean Netherlands (Bonaire, St Eustatius and Saba)).

Data transfer to a country outside of the Kingdom of the Netherlands is permitted, provided that the foreign country offers an appropriate degree of protection to personal data. Particular consideration must be given to:

- the nature of the data,
- the purpose and the duration of the intended processing,
- the country of origin and the country of final destination,
- the general and sectoral legal rules that apply in the foreign country, and
- the professional rules and the safety measures that are observed in the foreign country.

However, personal data can nonetheless be transferred to a foreign country in the following cases:

- (a) clear consent from the individual;
- (b) data transfer is necessary to implement an agreement between the individual and the controller, or for taking pre-contractual measures further to the individual's request that are necessary for concluding an agreement;
- (c) data transfer is necessary to conclude an agreement or perform an agreement that was already concluded between the controller and a third party in the interest of the individual;
- (d) data transfer is necessary for a substantial public interest or for the establishment, execution or defense of any right;
- (e) data transfer is necessary to safeguard the vital interests of the individual; or
- (f) data is transferred from a register established by law and which can be consulted by anyone or by any person who has a legitimate interest, provided that the statutory conditions for consultation are met in the case in question.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

It is advisable for individuals to be made aware about matters such as:

- (a) the kind of personal data that will be transferred,
- (b) to what party will the data be transferred,
- (c) where it will be stored, and
- (d) the type of protection that is offered for it.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Curaçao? Are there minimum standards? Does this differ by sector or size of the entity?

There must be appropriate technical and organizational measures to secure personal data against loss or wrongful processing. The Regulatory Authority of Curaçao (formerly the Curaçao Bureau for Telecommunication and Post) has issued guidelines in this regard. Also, recommendations pertaining to the GDPR can serve as a guideline.

9.2 How are personal data breaches regulated in Curaçao? What are the requirements for notification and response?

There is no legal obligation to report data breaches to the Commission for Protection of Personal Data, nor are there any requirements for responding to data breaches. However, the Commission for Protection of Personal Data can impose administrative enforcement measures, such as a restoration order to rectify the violation itself, or a fine. Individuals may also pursue civil or criminal enforcement.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) Administrative sanctions, such as the issuance of an enforcement order, or a fine of up to ANG 10,000 (approx USD 5,600);
- (b) Criminal sanctions such as a fine of up to ANG 10,000 (approx USD 5,600) or a prison sentence; and
- (c) Civil sanctions such as damages.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes. Remedies include:

- (a) damages;
- (b) a court order containing a prohibition on continuing the infringing behavior; and
- (c) a court order for the infringer to remedy the consequences of the violation of the Privacy Ordinance for the individual.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

There has been no action by enforcers because the Commission for Protection of Personal Data is not active.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Curaçao?

Curaçao is a relatively small community, and this motivates controllers and processors to observe extra due care in processing personal data.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

It is recommended to monitor 'hot topics' that are of international relevance, as these could give further context to local law provisions, as long as they do not conflict with local law.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

International practices that are standard across the board may be referenced to give further context to local law provisions, as long as these do not conflict with local law. Considering that the Privacy Ordinance is based on the Dutch Personal Data Protection Act (although the Dutch Personal Data Protection Act has now been replaced by the GDPR), Dutch standards and case law tend to be observed to interpret local privacy law. Also, the GDPR may apply in some cases, or may be observed as a guideline for good practice.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The intention is to submit the Privacy Ordinance to a full revision. Preparatory steps, including stakeholder consultation, have been taken, but the actual drafting process has not been initiated as yet. The revision of the Privacy Ordinance has been triggered by the ratification by the Netherlands of the Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), which requires a significantly higher level of protection than that provided by the Privacy Ordinance.

The Netherlands, Aruba and Sint Maarten are discussing the possibility of harmonizing privacy rules in a joint law, a so-called 'Consensus Kingdom Act', that will apply to them as countries of the Kingdom of the Netherlands. Curaçao is also a country of the Kingdom of the Netherlands, but has stated that it will not be part of the Consensus Kingdom Act on privacy.

More local companies and institutions are implementing a privacy policy, especially those that are active internationally or in certain sectors.

The Commission for Protection of Personal Data has not become active as yet.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Practical information on the implementation of measures to protect personal information.

12.3 What do you envision the privacy landscape will look like in five years?

- (a) Some practical guidelines about several topics may be made available to the public;
- (b) Changes in policies concerning artificial intelligence;
- (c) Hopefully, the Commission for Protection of Personal Data, that is in charge of supervising compliance with the Privacy Ordinance, will have become active.

 DOMINICAN REPUBLIC

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in the Dominican Republic.

Privacy is recognized as a fundamental right in the Constitution of the Dominican Republic, specifically stating: ‘Everyone has the right to privacy. Respect and non-interference in the private, family, and home life and to the correspondence of the individual is guaranteed.’ From this constitutional provision, several key principles derive:

- (a) the inviolability of the home;
- (b) the right to the protection of personal data; and
- (c) the inviolability of telecommunications secrecy.

In addition to the Constitution, Dominican courts have interpreted privacy rights in light of international human rights instruments, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Privacy is also regulated through special legislation, including laws on personal data protection and anti-spam, which reinforce individual rights and set limits on the use of personal information, particularly in commercial and technological contexts.

The Dominican Republic maintains a national legal framework that defines the rights of individuals over their personal data and imposes compliance obligations on public and private entities that process such information. Regulatory oversight is exercised by sector-specific authorities, and there is increasing emphasis on principles such as informed consent, transparency, and protection against unsolicited communications.

1.2 What are the primary laws regulating privacy in the Dominican Republic? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

In the Dominican Republic, privacy regulation is supported by a combination of constitutional provisions, statutory norms, and sector-specific legislation. At its foundation, the Constitution recognizes privacy as a fundamental human right. It guarantees the inviolability of private, family, and home life, and explicitly safeguards the confidentiality of telecommunications and the right to the protection of personal data. The Constitution also grants individuals the ability to access, rectify, and delete their personal information held by both public and private entities. Dominican courts have reinforced these protections by interpreting them in light of international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Building upon this constitutional guarantee, Law No 172-13 on the Protection of Personal Data (‘Personal Data Protection Law’) constitutes the central legislative framework governing data privacy. The law mandates that personal information may only be collected and processed with prior, informed consent and establishes key rights for individuals, such as the ability to access, update, and object to the use of their data. It also imposes legal obligations on data controllers—whether public or private—to implement security measures that preserve confidentiality and prevent unauthorized access.

In the domain of advertising and electronic communications, privacy is addressed through Law No 310-14 (‘Anti-Spam Law’). This law prohibits the distribution of unsolicited promotional messages via email, SMS, and other digital channels unless the recipient has expressly opted in. The enforcement of

this provision falls under the jurisdiction of the national telecommunications regulator, INDOTEL. While there exists an advertising self-regulation code developed by private sector actors—which outlines principles related to personal dignity and privacy—it currently lacks binding authority and is not actively enforced.

Further privacy protections are found in Law No 53-07 on High-Tech Crimes (‘Cybercrime Law’), which criminalizes unauthorized access to personal data and the interception or alteration of digital communications. The Criminal Procedure Code complements these safeguards by requiring judicial authorization for any interception of private communications within criminal investigations.

From a consumer rights perspective, Law No 358-05 (‘Consumer Protection Law’) plays a significant role. Administered by the national consumer protection agency, ProConsumidor, this law regulates how personal data can be used in commercial settings. It prohibits misleading or deceptive advertising and obligates businesses to provide clear and transparent information when handling consumers’ data, particularly in online environments. Additionally, the regulation of e-commerce is reinforced through various technical norms and resolutions issued by INDOTEL, covering electronic contracting, digital authentication, and cybersecurity obligations for online service providers.

Privacy in the Dominican Republic is also protected in the context of personal image rights. A specific statute prohibits the unauthorized publication or distribution—via traditional or digital media—of images of individuals who are deceased or injured in accidents, unless prior authorization is obtained. This law seeks to preserve the dignity and privacy of the individuals involved and their families, particularly in news or public communications.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In the Dominican Republic, self-regulation plays only a minimal role in privacy protection within the advertising sector. The Dominican Commission of Advertising Self-Regulation (‘CODAP’) was established to promote ethical standards in advertising, including respect for personal data and individual likenesses. However, despite the existence of a self-regulatory code that outlines responsible practices, CODAP has not been fully implemented, and the code lacks binding legal authority or enforcement mechanisms. As a result, its practical impact on privacy protection remains limited and largely aspirational, serving more as a reference framework than an operative system of oversight.

1.4 How is privacy law enforced in the Dominican Republic? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

There is no designated data protection authority in the Dominican Republic. Instead, privacy rights are enforced through the courts in civil and constitutional matters. However, despite the absence of a dedicated data protection body, ProConsumidor has played an increasingly active role in safeguarding personal data, particularly in cases where the processing of such data presents clear risks to fundamental rights.

In terms of enforcement mechanisms, the Office of the Public Prosecutor (District Attorney) and the National Police are responsible for applying the law when a criminal offense has been committed—for example, in cases of unlawful interception, surveillance of data transmissions or telecommunications, or unauthorized access to databases. The Public Prosecutor also has jurisdiction over violations of the

Personal Data Protection Law, including unauthorized access to or consultation of data held by credit bureaus.

Additionally, the Superintendency of Banks, which oversees the operation and compliance of financial institutions, holds regulatory authority over the personal data practices of credit information bureaus. However, current legislation does not require credit bureaus to register their databases or to notify authorities when data is transferred, limiting the scope of oversight in this sector.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in the Dominican Republic?

Generally speaking, all individuals and legal entities—including companies—are subject to privacy legislation in the Dominican Republic when they collect, store, process, or transfer personal data of individuals, whether those individuals are consumers, clients, employees, or third parties. The Personal Data Protection Law applies broadly to both public and private entities that handle personal data within the national territory.

In addition to this general framework, certain sectors are governed by specific rules and regulatory oversight. For example, credit bureaus (also referred to as credit reporting agencies) are subject to detailed obligations under the Personal Data Protection Law, including requirements for data accuracy, prior consent, and individuals' rights to access and correct their personal information. In the financial services sector, both the Superintendency of Banks and ProUsuario (the consumer protection office for users of financial services) monitor compliance with data handling obligations, particularly regarding credit and transactional information. In the telecommunications sector, companies must comply with privacy and anti-spam regulations issued by INDOTEL and are subject to supervision by its Dirección de Protección al Usuario ('DPU'), which oversees the protection of user rights in electronic communications, including the confidentiality of personal data and the proper use of customer information.

2.2 Does privacy law in the Dominican Republic apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Unlike other privacy frameworks like the GDPR, the Personal Data Protection Law does not contain a specific article with extraterritorial scope. The law is territorial in focus, and its obligations clearly apply to:

- (a) controllers or processors domiciled in the Dominican Republic, and
- (b) databases located within the territory of the Dominican Republic.

This means that only foreign companies with a physical or legal presence in the Dominican Republic (eg, a branch, office, or subsidiary) are directly subject to Dominican Law when processing personal data locally. Also, foreign companies operating through Dominican-based databases or infrastructure are also subject to the law by implication.

In consequence, the Personal Data Protection Law does not expressly apply to foreign companies without a local presence or infrastructure, such as purely online platforms based abroad that collect data from Dominican users remotely.

It is important to note that Dominican Law also does not mandate the appointment of a local representative for foreign companies, nor does it create an express legal mechanism for extraterritorial enforcement.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in the Dominican Republic?

The Personal Data Protection Law defines ‘personal data’ as: ‘Any numerical, alphabetical, graphic, photographic, acoustic, or other type of information concerning identified or identifiable natural persons.’

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Categories of personal data considered sensitive in the Dominican Republic include a person’s political opinions, religious beliefs, philosophical or moral convictions, labor or union affiliation, and information related to health or sexual life. While racial origin is not formally listed in the core definition of sensitive data, it is referenced as a protected category in specific exceptions related to health treatment and medical services (see below).

Under the Personal Data Protection Law, the processing of sensitive personal data is generally prohibited unless the data subject provides express, free, and informed consent. Entities handling such data must obtain this explicit consent prior to any use, collection, or processing.

There are two main exceptions to the rule requiring express consent and the general prohibition on processing:

- (i) Religious organizations, hospitals, political parties, and labor unions are allowed to collect and process sensitive data for the purposes of maintaining membership registries or fulfilling their institutional mandates; and
- (ii) Sensitive data concerning health, racial origin, or sexual life may be processed when necessary for the prevention, diagnosis, or treatment of medical conditions, or for the management of healthcare services—provided that the data is handled by professionals subject to legal obligations of confidentiality or professional secrecy.

Sensitive data is subject to stricter protection under Dominican law. Key distinctions include:

- (a) **Explicit consent:** The data subject must give explicit and informed consent prior to the processing of sensitive data. General or implied consent is not sufficient;
- (b) **Purpose limitation:** Sensitive data can only be processed for specific, legitimate, and necessary purposes, and not for general or undefined uses;
- (c) **Prohibition on processing:** In general, the processing of sensitive data is prohibited unless the data subject has given consent, or the processing is authorized by a specific legal exception (eg, for medical treatment, public health, or legal obligations);
- (d) **Stronger security measures:** Data controllers must implement heightened security safeguards when handling sensitive data to prevent unauthorized access, loss, or misuse; and
- (e) **Risk of civil and criminal liability:** Unlawful processing or disclosure of sensitive data may lead to civil damage and, in some cases, criminal penalties under the Cybercrime Law.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The Dominican Republic's Personal Data Protection Law does not use the international terminology of 'anonymized,' 'pseudonymized,' or 'de-identified' data. However, it recognizes a similar concept under the term 'disociación'.

Disociación refers to the processing of personal data in such a way that the resulting information cannot be associated with a specific or identifiable person. This aligns with the idea of anonymization in other privacy frameworks. Data that has been effectively disassociated in this manner is generally no longer subject to the obligations of the law, since it is no longer considered personal data.

Additionally, the law authorizes data controllers to apply disassociation procedures when identification of individuals is no longer necessary for the intended processing purpose. This provision supports the principle of data minimization, encouraging the use of non-identifiable data when feasible.

By contrast, the law does not explicitly address pseudonymization, ie, situations where data is masked but could still be re-linked to an individual. In the absence of explicit provisions, such data would likely still be considered personal data under Dominican law, because the individual remains potentially identifiable.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Under the Personal Data Protection Law, companies operating in the Dominican Republic that collect, store, or otherwise process personal data are subject to a set of fundamental legal obligations as follows, aimed at ensuring transparency, safeguarding individual rights, and promoting responsible data management:

- (a) Personal data must be processed lawfully, fairly, and for specific, legitimate purposes.
- (b) Data subjects must be clearly informed about the purpose of data collection, the identity and address of the data controller, and their rights, including access, correction, opposition, and deletion.
- (c) Express, prior, and informed consent is required—especially for sensitive data—and such consent must be documented and revocable.
- (d) Data quality and minimization must be ensured, meaning data must be accurate, kept up to date, and collected only to the extent necessary for the intended purpose.
- (e) Security and confidentiality are mandatory, requiring companies to adopt both technical and organizational safeguards to prevent unauthorized access, alteration, or loss.

Furthermore, individuals have enforceable rights to access their personal data, request rectification, object to certain uses, and demand erasure when the data is no longer necessary or was processed unlawfully.

International data transfers are restricted unless the receiving country ensures an adequate level of data protection, or unless specific legal exceptions—such as data subject consent—apply. See question 8.1.

Although not explicitly required under Dominican law, it is considered best practice for companies to maintain internal data protection protocols, including employee training and voluntary record-keeping. The law does not require the appointment of a data protection officer.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The Personal Data Protection Law does not explicitly distinguish between ‘data controller’ and ‘data processor’ using those exact terms. However, from the structure and language of several provisions—particularly those referring to the ‘responsable del banco de datos’—we can infer a functional distinction that aligns with the concepts of controller and processor found in other privacy regimes, such as the GDPR.

The ‘responsable del banco de datos’—the person or entity responsible for the data file—corresponds to the role of a data controller, as this entity determines the purposes and means of processing personal data. Although the law does not formally define a category for data processors, it anticipates the participation of third parties in data processing activities and imposes duties of confidentiality and lawful handling, thereby implying processor-like responsibilities. In this way, the Dominican legal framework recognizes different levels of responsibility depending on an entity’s role in the data lifecycle, even if the terminology remains undeveloped.

The controller or ‘responsable del banco de datos’ must ensure that such processors guarantee confidentiality, legal compliance, and adequate security.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, Dominican privacy law requires a lawful basis for processing personal data. Under the Personal Data Protection Law, the primary legal basis is prior, express, and informed consent from the data subject. This consent must be obtained before collecting or processing personal data, and individuals must be clearly informed of the purpose, the identity of the data controller, and potential recipients.

While the law does not establish ‘legitimate interest’ as a general, independent basis for all processing, the concept is recognized in the context of personal data transfers—particularly when the transfer serves the legitimate interests of both parties, or is made at the request of an international organization.

One specific marketing exception to the general requirement for consent for the processing and transfer of data is when it comes to lists for marketing purposes, where data are limited to name, identity and electoral card, passport, tax identification and other biographical information.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

In the Dominican Republic, the Personal Data Protection Law requires that companies provide a clear and express privacy notice whenever they collect personal data—including for advertising purposes—especially when the processing relies on the data subject’s consent. The law applies equally to public and private entities, and the same core transparency obligations apply, regardless of the processing purpose. The following information, inter alia, should be included:

- (a) **Purpose of the data processing:** Companies must clearly inform the individual of the specific purpose for which the personal data will be used, such as marketing, promotional communication, or targeted advertising;
- (b) **Identity and address of the data controller:** The notice must specify who is collecting the data and where they are based (ie, the name and domicile of the responsible entity);
- (c) **Recipients or categories of recipients:** It must disclose who will have access to the data, or the categories of third parties to whom the data may be transferred (eg, marketing agencies, affiliates); and
- (d) **Existence of a data file or database:** The notice must indicate whether the data will be incorporated into a structured system.

Personal data processed by governmental entities must also indicate the services or units before which the rights of access, rectification, cancellation and opposition may be exercised.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

In the Dominican Republic, consumers enjoy a set of privacy rights concerning the use of their personal data in advertising contexts, primarily governed by the Personal Data Protection Law and complemented by the Anti-Spam Law:

- (a) Under the Personal Data Protection Law companies must obtain the consumer's prior, express, and informed consent before collecting or using personal data for marketing purposes. This includes informing individuals of the specific purpose for the data collection, the identity and address of the data controller, and any third parties or categories of recipients. Consumers also hold the rights to:
 - (i) access their data,
 - (ii) rectify inaccuracies,
 - (iii) object to data use for advertising, and
 - (iv) request deletion when data is no longer necessary or was processed unlawfully.
- (b) The Anti-Spam Law reinforces these protections specifically for electronic marketing communications, establishing the following key privacy rights:
 - (i) **Right to prior consent (Opt-In Requirement):** Companies must obtain explicit prior consent before sending promotional emails, SMS, or similar digital messages.
 - (ii) **Right to withdraw consent (Opt-Out):** Consumers must be offered clear and accessible options to unsubscribe from future communications.
 - (iii) **Right to be free from unsolicited messaging:** The law prohibits the massive or indiscriminate sending of advertising messages without prior authorization, protecting individuals from privacy intrusions.
 - (iv) **Right to transparency:** Marketing messages must clearly indicate their commercial nature and identify the sender to avoid misleading the recipient.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

We must begin by noting that companies are required to obtain consent or provide opt-out options for advertising activities in specific circumstances, as established by the Personal Data Protection Law and the Anti-Spam Law. These legal frameworks mandate that companies process personal data for advertising purposes in a transparent, lawful, and respectful manner.

With regard to opt-out mechanisms, all promotional communications must include a clear, visible, and easily accessible option that enables recipients to opt out or unsubscribe from future advertising messages. This mechanism must be straightforward and fully functional.

Furthermore, upon the withdrawal of consent—whether expressed verbally or in writing—the company must immediately cease any further use of the individual’s personal data for promotional purposes.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

While the Personal Data Protection Law does not expressly name actors such as advertising agencies, data providers, or digital advertising platforms (eg, DSPs and SSPs), it clearly establishes obligations that apply whenever personal data is shared with or processed by third parties for advertising purposes.

Dominican law imposes general obligations on any entity that handles personal data. When advertisers engage external partners for data-driven campaigns, the following apply:

- (a) **Consent-based sharing:** Personal data may only be shared with third parties—including vendors or agencies—if the data subject has provided prior, express, and informed consent, including consent for the personal data to be transferred. This means companies must disclose the potential sharing of data with external entities and obtain consent before such transfers.
- (b) **Purpose limitation and legitimate interest:** Dominican Law allows data transfers only when they are directly related to the legitimate interest of both the transferring and receiving party, and for clearly defined purposes. This limits how vendors and platforms may repurpose data for broader or unrelated advertising uses.
- (c) **Third-party obligations and confidentiality:** Companies must ensure that any third-party processors (even if not formally distinguished as such in the law) adhere to principles of confidentiality, data security, and lawful processing. The law implicitly imposes a duty on the original data controller to supervise how data is used downstream.
- (d) **No explicit contracts required:** Dominican law does not expressly require data processing agreements (‘DPA’s) between the data controller and third parties. However, it is considered best practice to have written agreements that bind vendors to data protection obligations.
- (e) **Accountability of the primary data controller:** The primary data controller (ie, the entity originally collecting the data) remains legally responsible for how personal data is processed, even when it is handled by third parties.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

In the Dominican Republic, the Personal Data Protection Law does not impose detailed or explicit requirements for contractual arrangements between companies (data controllers) and vendors or other third parties (such as data processors). However, the law establishes substantive obligations that imply the need for responsible handling of personal data in such relationships. These substantive obligations include, for example, as indicated above, obtaining prior consent, ensuring purpose limitation, and safeguarding confidentiality and security.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

In the Dominican Republic, privacy due diligence obligations are not as prescriptive as in jurisdictions such as the European Union under the GDPR. However, under the Personal Data Protection Law, companies are expected to undertake reasonable and responsible practices when collecting, processing, and sharing personal data—including for advertising purposes. Thus:

- (a) **Due diligence expectations:** While the law does not mandate formal ‘privacy impact assessments’, companies are implicitly expected to:
 - (i) obtain prior, informed, and express consent from data subjects before collecting or using personal data, particularly for advertising and profiling purposes;
 - (ii) ensure data minimization and purpose limitation, meaning that only relevant data should be collected and used strictly for clearly stated purposes;
 - (iii) verify that third-party vendors or processors (eg, advertising agencies or data platforms) comply with confidentiality, security, and lawful processing standards;
 - (iv) implement technical and organizational measures to prevent unauthorized access, loss, or misuse of personal data; and
 - (v) respond to data subject requests, such as access, rectification, or deletion of data.
- (b) **Impact assessments:** The Personal Data Protection Law does not include a formal requirement for privacy impact assessments (‘DPIA’s)—even for high-risk data processing activities such as targeted advertising or profiling. However, companies are expected to assess the legal basis, risks, and safeguards before initiating data-intensive advertising practices, especially if sensitive data is involved.

In the absence of a mandatory DPIA framework, businesses engaging in data-driven advertising should still document internal assessments to demonstrate compliance with principles of consent, purpose limitation, and data security—especially in case of future investigations or civil claims.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Anti-Spam Law expressly grants users in the Dominican Republic the right not to receive unsolicited commercial emails containing advertising or promotional offers (ie, spam). Users also have the right to reject such emails and to opt out of any mailing list to which they had previously consented.

However, companies may lawfully send commercial, promotional, or advertising emails if there is an existing commercial relationship with the recipient. In all cases, the collection of email addresses must be conducted legally and transparently—the malicious harvesting or scraping of email addresses is expressly prohibited under Dominican law.

All marketing emails must be clearly identified as ‘advertising’ (‘publicidad’) and must include:

- (a) the identity of the sender, and
- (b) a valid return address or reply mechanism that allows recipients to opt out of future communications.

Importantly, these obligations apply exclusively to email communications and do not extend to marketing through social media platforms, which remain outside the scope of the Anti-Spam Law.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Under Dominican privacy law, specifically the Personal Data Protection Law, there is no specific regulation that expressly addresses tracking technologies such as cookies, pixels, SDKs, or similar digital tools used for user profiling and behavioral advertising.

However, general data protection principles do apply to tracking technologies when they involve the collection or processing of personal data, such as IP addresses, browsing behavior, location data, or device identifiers.

7.3 How are loyalty programs and promotions regulated under privacy law?

In the Dominican Republic, loyalty programs and promotional campaigns are not expressly regulated under the Personal Data Protection Law, but they are subject to its general principles and obligations when they involve the collection or use of personal data.

ProConsumidor enforces data protection clauses in the rules of promotions, raffles and games.

7.4 How is social media and influencer marketing regulated under privacy law?

In the Dominican Republic, social media and influencer marketing are not subject to a dedicated law; however, they are regulated indirectly through privacy, advertising, and consumer protection laws, especially when personal data is collected, used, or shared in the context of these activities.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

The Dominican Republic's Personal Data Protection Law permits the use of personal data for advertising, direct marketing, and profiling activities—such as those commonly associated with targeted or behavioral advertising—under specific conditions. Companies are allowed to compile addresses and other personal information to establish consumer profiles for promotional or commercial purposes, provided that the data originates from publicly accessible sources, is voluntarily provided by the individuals themselves, or is collected with their consent.

This legal framework enables organizations to analyze consumer habits and preferences to deliver more personalized advertising, while also ensuring that individuals retain key privacy rights. These include the right to access their personal data at no cost and the ability to request the removal or blocking of their information from marketing databases at any time. As a result, the law supports data-driven marketing practices while reinforcing individual autonomy and transparency in how personal data is used for advertising purposes.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

In the Dominican Republic, digital identity resolution and clean room technologies are not explicitly regulated under existing privacy laws. However, these technologies—because they often involve the collection, combination, or processing of personal data from multiple sources—are indirectly subject to the core principles and obligations established by Dominican laws.

7.7 How is location-based advertising regulated under privacy law?

In the Dominican Republic, location-based advertising is not explicitly regulated as a distinct category under privacy laws. However, the general principles of data protection apply fully when location data is used to identify or target individuals.

7.8 How are data brokers defined and regulated under privacy law?

The Personal Data Protection Law does not explicitly define or regulate ‘data brokers’ as a distinct category. However, the law’s provisions apply to any individual or entity that collects, stores, processes, or transfers personal data, including those that trade in or aggregate such information for commercial purposes.

7.9 How is advertising to children and minors regulated under privacy law?

While the Personal Data Protection Law does not include a dedicated section on children’s data, it requires that all processing of personal data be carried out with lawful, fair, and informed consent—conditions that are especially stringent when dealing with sensitive or vulnerable groups, such as minors. In practice, this implies that any use of a minor’s personal data for advertising purposes should be preceded by the express, informed, and verifiable consent of a parent or legal guardian.

Additionally, Law 136-03 on child protection contains broader provisions that prohibit practices which exploit, manipulate, or otherwise negatively affect the integrity or development of minors. It emphasizes the right of children and adolescents to be protected from all forms of exploitation, including through advertising that may be misleading, inappropriate, or that targets them unfairly. The law also reinforces the principle that the best interest of the child must always prevail in any situation involving commercial communication or data processing that includes minors.

Taken together, these legal provisions suggest that companies must exercise heightened diligence, transparency, and care when designing advertising strategies aimed at or involving children in the Dominican Republic.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

In the Dominican Republic, privacy law does not contain specific or express provisions regulating the use of artificial intelligence (‘AI’), profiling, or automated decision-making technologies for advertising purposes.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes, the Personal Data Protection Law imposes restrictions on cross-border transfers of personal data. These transfers are subject to specific safeguards designed to ensure that individuals’ privacy rights are not undermined when their data is processed outside the country as follows:

- (a) **Conditions for international data transfers:** According to the law, personal data may only be transferred internationally if the receiving country provides an adequate level of data protection that is ‘comparable’ to Dominican standards. The adequacy of protection must relate to how the data will be processed, the type of data, and the applicable legal guarantees.

- (b) **Exceptions allowing transfers without adequacy:** Transfers may still take place even if the recipient country lacks adequate protection, provided that:
 - (i) the data subject has given express and informed consent;
 - (ii) the transfer is necessary for the execution of a contract with the data subject or in their interests;
 - (iii) the transfer is legally required under international treaties or to safeguard the public interest;
 - (iv) the transfer is made to an international organization that follows protective data handling practices.
- (c) **Standard clauses or agreements:** While the Personal Data Protection Law does not explicitly refer to standard contractual clauses ('SCC's) as required under the GDPR, contracts or binding agreements that impose adequate data protection obligations on the foreign recipient may be used as a legal safeguard for data transfer approval. However, the law does provide a related and potentially analogous mechanism. It enables both public and private data controllers—and their sectoral or organizational groups—to develop model codes that define internal practices, operational standards, security measures, and procedures regarding the handling of personal data.
- (d) **Prohibited transfers:** The law does not publish a formal list of prohibited jurisdictions but empowers the data authority (or courts) to object to transfers if the recipient country fails to meet the required level of protection and no valid exception applies.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Yes, under the Personal Data Protection Law there are additional considerations for personal data transfers beyond general consent and adequate destination safeguards. Transfers of confidential or privileged data—such as medical, legal, or financial information—require strict handling and often need express authorization or a legal basis. Medical records, for instance, may only be transferred by professionals bound by confidentiality obligations, and legally privileged data may not be disclosed without proper legal grounds.

Transfers may also occur without consent if required by law, for reasons of public interest (such as health or security), or in compliance with international treaties. In all cases, individuals must be informed of transfers, especially to third countries, and retain their rights to access, object, or request deletion of their data. Finally, sensitive data (eg, health, political views, biometrics) are subject to stricter consent requirements and may only be transferred under limited, lawful conditions.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in the Dominican Republic? Are there minimum standards? Does this differ by sector or size of the entity?

In the Dominican Republic, data security is regulated under the Dominican Constitution that expressly mandates data security as a legal principle in the processing of personal data. This establishes a clear constitutional basis for requiring organizations to implement measures that safeguard personal data against unauthorized access, loss, or misuse, and reinforces the broader framework under the Personal Data Protection Law, which establishes general obligations for public and private entities to implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration, or disclosure.

While the law does not prescribe specific technical standards (such as encryption protocols or minimum cybersecurity benchmarks), it emphasizes the duty of confidentiality and the responsibility of data controllers and processors to preserve the integrity and security of personal information.

The law requires that personal data be stored in a way that guarantees its authenticity, confidentiality, and integrity, particularly when sensitive data is involved. However, it does not differentiate obligations based on the size of the entity or the volume of data processed. Instead, sectoral regulations impose additional standards, for example on financial institutions and telecommunications providers.

9.2 How are personal data breaches regulated in the Dominican Republic? What are the requirements for notification and response?

In the Dominican Republic, the Personal Data Protection Law does not establish explicit requirements for mandatory data breach notification. There are no prescribed deadlines, reporting formats, or formal obligations for notifying supervisory authorities or affected individuals in the event of a data breach.

Outside of the banking and credit reporting sectors, where specific obligations may apply under financial or sectoral regulations, there are no concrete legal requirements for incident response or breach disclosure. For most entities, the law imposes only a general obligation to preserve the integrity, confidentiality, and security of personal data. This includes adopting technical and organizational measures to protect the data under their control, but no sanctions apply solely for the occurrence of a breach, unless it involves unlawful conduct.

However, where a data breach results from unauthorized access, interception, or disclosure of personal data—for example, through hacking or insider misconduct—criminal penalties may apply under the Cybercrime Law. This law penalizes illicit access to computer systems, unauthorized disclosure of data, and other technology-related offenses.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

In the Dominican Republic, violations of privacy law may lead to both civil and criminal liability. The Personal Data Protection Law does not create a specific administrative authority for enforcement, and there is no general system of administrative fines. Instead, compliance is primarily ensured through the courts and certain sectoral regulators.

Companies and individuals that unlawfully collect, use, or disclose personal data may face civil lawsuits from affected individuals. Courts can award damages for unauthorized processing, failure to respect data subject rights, or breaches of data security and confidentiality. Compensation may cover both material harm and emotional distress.

The Personal Data Protection Law also includes criminal penalties. Offenses such as falsifying data, illegally accessing databases, or disclosing personal information without consent can result in prison sentences ranging from six months to two years and fines equivalent to 100 to 150 times the minimum wage. These penalties apply whether the violation is committed by an individual or a company representative.

Additional enforcement exists for credit bureaus, which are overseen by the Superintendency of Banks. In this sector, fines of up to USD 30,000 may be imposed for violations related to the handling of personal data.

Separately, the Cybercrime Law applies to privacy breaches involving unauthorized access, data interception, or digital misuse. Individuals found guilty under this law may face prison terms of one to three years and monetary fines, depending on the severity of the offense.

Although enforcement is still developing, these provisions show that data protection in the Dominican Republic is supported by both civil remedies and criminal enforcement mechanisms.

10.2 Do consumers have a private right of action? What remedies are available to them?

The Dominican Law admits the habeas data personal action to enforce the Personal Data Protection Law. It entitles individuals to collect, rectify or delete their personal data.

Victims are entitled to civil damages, specifically in cases of:

- (a) denial, without foundation, of a request for revision or an application for rectification of the credit information required by the information holder;
- (b) refusal to modify or delete the information of data subjects, after they have obtained a favorable pronouncement in a procedure followed in accordance with the provisions of the Personal Data Protection Law; or
- (c) serious or repeated violation of the provisions of definitive sentences of the civil courts.

If the privacy violation has been committed alongside a violation of the Cybercrime Law (eg, illegal access), penalties are much higher.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

There has been no enforcement against privacy non-compliance involving advertising.

Outside advertising, in 2024, ProConsumidor intervened against the operations of the company Worldcoin, ordering it to cease activities and delete biometric data that had been collected without sufficient legal safeguards. The company challenged the measure in court, but the Administrative Superior Court rejected the request for injunctive relief, thereby affirming the legitimacy of ProConsumidor's authority in this matter. This case demonstrates that, in the absence of a specialized data protection regulator, certain sectoral agencies are beginning to assume de facto responsibilities for data privacy, especially when closely connected to consumer protection.

Enforcement has also occurred through the constitutional courts, where individuals have filed 'acción de amparo' (constitutional writs) to demand deletion or correction of personal data—mainly in credit and financial contexts. However, no major precedents exist involving privacy violations related to targeted or digital advertising.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in the Dominican Republic?

Sadly, it is very common in the Dominican Republic for companies and government institutions to require personal data from individuals. In a high percentage of these cases, data is collected without notification or meeting the requirement of authorization for data treatment and transfer.

Despite high rates of smartphone and social media use, public understanding of data protection rights remains limited. Many individuals voluntarily share personal and even sensitive data online without concern for legal implications, which weakens societal demand for stronger enforcement or comprehensive reform.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

The Government has prepared a new draft data protection law closely modelled on the GDPR.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Judicial Branch (Poder Judicial) in the Dominican Republic approved a data protection policy in October 2023. It represents a major step forward in governmental data protection practices—emphasizing anonymization, database minimization, and the data subject’s rights to privacy. It’s an exemplary model for other public institutions in the Dominican Republic to move toward stronger privacy compliance.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Dominican Republic privacy law has moved beyond 2022’s largely declarative framework. New judicial policy, regulatory drafts, and high-profile interventions signal a proactive shift—especially in handling sensitive data and digital content. Companies should monitor these and anticipate further government-led reforms, stronger enforcement mechanisms, and broader protections in areas like AI, profiling, and breach notification.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

One of the biggest challenges companies face in the Dominican Republic is the outdated nature of the current privacy framework, which significantly limits their ability to compete in a global, data-driven economy. While the Personal Data Protection Law establishes foundational rights and obligations, it does not address modern principles, such as privacy by design, nor does it offer uniform implementation guidelines for integrating privacy into systems, platforms, or software development lifecycles.

This regulatory gap creates considerable uncertainty for companies seeking to innovate responsibly—particularly in industries that rely on behavioral data, artificial intelligence, or cross-border

processing. Unlike jurisdictions with more advanced data protection regimes, Dominican law lacks clearly defined exemptions, compliance pathways, or standardized best practices for emerging technologies, leaving organizations without reliable models to emulate.

As a result, businesses often struggle to design compliant products and services from the outset, face higher legal risk, and may find themselves at a disadvantage in international markets that demand greater accountability and transparency in data processing. The absence of modern rules and practical guidance ultimately hinders both technological competitiveness and consumer trust.

12.3 What do you envision the privacy landscape will look like in five years?

In practice, although the enforcement of privacy provisions in the Dominican Republic continues to evolve, businesses engaging in modern advertising practices—such as targeted campaigns via social media, mobile apps, geolocation services, and tracking technologies—should adopt a privacy-by-design approach. This means incorporating data protection safeguards from the outset of any advertising initiative, ensuring transparency, limiting data collection to what is strictly necessary, and securing valid consent where required.

As digital advertising grows increasingly sophisticated—relying on profiling, personalization, and real-time behavioral data—the Dominican Republic must move sooner rather than later toward enacting a more complete and comprehensive privacy and data protection framework. While the Personal Data Protection Law and related sectoral norms provide a basic structure, they fall short in addressing the complex realities of today's data-driven marketing ecosystem. A modernized legal framework is essential, not only to safeguard individual rights more effectively, but also to provide legal certainty for businesses operating in an increasingly competitive digital environment.

 ECUADOR 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Ecuador.

The Ecuadorian Constitution of 2008 recognizes and guarantees the protection of personal data, establishing that the owner's authorization is required for any collection, storage or dissemination of personal information.

Furthermore, the data protection landscape changed on May 26, 2021, when the Organic Law of Personal Data Protection ('LOPDP') was published in the Official Gazette, providing an effective legal framework for the exercise of privacy rights in Ecuador. Subsequently, the General Regulations to the LOPDP were issued on May 26, 2023, establishing specific guidelines for implementation of the law.

For the supervision and enforcement of the law and regulations, the Superintendence of Personal Data Protection ('Superintendence') was created, an entity that has the power to issue regulations, supervise compliance of the LOPDP and sanction data protection violations. With the creation of the Superintendence and the appointment of its first Superintendent in June 2023, Ecuador now has a competent authority in charge of guaranteeing the effective exercise of the rights of personal data owners. However, significant challenges remain in the effective implementation of the regulation, including the need to strengthen oversight, raise awareness of the right to privacy and consolidate the practical application of the provisions established in the law.

1.2 What are the primary laws regulating privacy in Ecuador? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The main laws regulating privacy in Ecuador include:

- (a) **Constitution of the Republic of Ecuador:** This recognizes the fundamental right to the protection of personal data and establishes principles of privacy and informational self-determination. Article 66 guarantees the right to data protection, while Article 92 determines that the authorization of the owner of the data is required both for its collection and dissemination;
- (b) **LOPDP:** This is the main law on privacy and establishes the rights of data owners, the categories of data, the obligations of data controllers and data processors, as well as various provisions that make up a comprehensive legal framework for the protection of privacy in Ecuador;
- (c) **General Regulation to the LOPDP:** This details the practical implementation of the LOPDP and the supervision and sanction mechanisms, including rules on the use of personal data in the commercial and advertising fields;
- (d) **Civil Code:** Within the framework of contractual relations, this regulates aspects related to confidentiality and data processing between private parties;
- (e) **Law on Electronic Commerce, Signatures and Data Messages:** This regulates the collection and use of data in digital commerce and establishes obligations in electronic advertising;
- (f) **Organic Law of Jurisdictional Guarantees and Social Control:** This establishes the habeas data action, in accordance with the Constitution;
- (g) **Organic Telecommunications Law:** This regulates the rights of users of telecommunications services, the obligations of the providers of these services, the right to privacy and the commercial use of personal data;

- (h) **Organic Law of Communication:** This establishes principles on the responsible use of information in media and advertising, promoting the protection of personal data in the sector;
- (i) **Regulation for filing Complaints and Requests issued by the Superintendence:** This defines administrative procedures for complaints related to the protection of personal data;
- (j) **Circular 2024-005-OC:** This establishes guidelines on the delegation of personal data protection in public institutions; and
- (k) **Technical Guide for the Registration of Special Proxies:** This establishes regulations on special proxies, their designation and registration at a national level.

1.3 **What role does self-regulation play in privacy regulation, particularly for advertising practices?**

The LOPDP imposes specific self-regulation obligations and has a whole chapter focused on proactive responsibility, including dispositions on codes of conduct and certification entities. Furthermore, self-regulation in Ecuador has become relevant in sectors such as advertising and telecommunications. The Organic Law of Communication establishes that the media and companies in the sector regulate their behavior through codes of ethics and editorial policies. In the advertising sector, this allows companies to adopt standards of transparency in the use of personal data and to apply privacy principles from the design stage. The principle of ‘social sensitivity’ seeks to balance freedom of expression with the protection of citizens’ rights, promoting self-regulation in the handling of personal information in media and advertising.

Likewise, the Organic Law of Telecommunications protects the privacy of users of telecommunications services and limits the use of their data for commercial purposes without their consent. This has driven the implementation of opt-out practices and the use of anonymized data in digital advertising. In addition, the law establishes the rights of customers and users regarding the protection of their personal data, thus strengthening the responsibility of companies in the processing of information for commercial purposes.

Together, these regulations allow self-regulation to complement government oversight, promoting internal standards and compliance mechanisms in the advertising industry. In the advertising sector, self-regulation allows companies to establish transparent data collection and use practices, such as providing accessible opt-out mechanisms and adopting privacy principles by design.

1.4 **How is privacy law enforced in Ecuador? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.**

Compliance with the LOPDP is supervised by the Superintendence, who has the power to conduct audits, issue sanctions and establish technical guidelines for the application of the regulations. However, to date there have been no cases of sanctions in this area, as the Superintendence is still in the process of consolidation and regulation. In addition, data subjects have the right to file complaints before the Superintendence if they consider that their rights have been violated, although challenges remain in the effective implementation of these mechanisms. They can also bring legal action in case of misuse of their data, which could eventually result in financial penalties or corrective measures. The regulatory framework is still under development, and the practical application of sanctions and resolutions by the Superintendence will depend on the evolution of its operational structure and the creation of jurisprudence on the matter.

At the enterprise level, companies can implement internal compliance mechanisms, such as privacy impact assessments, security audits and the appointment of data protection officers ('DPO's), to ensure regulatory compliance and minimize legal risks. Furthermore, the LOPDP establishes the obligation to appoint a DPO on all companies from the public sector, and those processing of data involved with national security and 'large scale' processing. 'Large scale' processing is defined as:

- (a) The processing of patient data in the normal course of business of a hospital, or of the institutions that make up the National Health System;
- (b) The processing of travel data of persons using the public transportation system of a city (eg, tracking through transportation cards);
- (c) The processing of real-time geolocation data of customers by a personal data controller specialized in the provision of these services;
- (d) The processing of customer data in the normal course of business of an insurance company, brokers, agents, lenders or financial institutions;
- (e) The processing of personal data for behavioral advertising by a search engine; and.
- (f) The processing of data (content, traffic, location) by telephone or internet service providers.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Ecuador?

According to the Constitution and the LOPDP, any entity, public or private, is subject to the Law when it processes data of any natural person in the Ecuadorian territory or abroad (for people who reside in Ecuador) when the processing activities are related to:

- (a) the offering of goods or services to such individuals, regardless of whether they are required to pay for them; or
- (b) the monitoring of their behavior, to the extent that this takes place in Ecuador.

The Law is applicable to the processing of personal data contained in any type of support (ie, whether processed by electronic or physical devices), except for cases such as domestic activities, anonymized data, journalistic activities, data related to criminal offenses and data that identifies companies. As the names, functions, address and phone numbers of professionals, public servants, companies' legal representatives and shareholders are accessible to the public, they are available for processing without prior consent.

2.2 Does privacy law in Ecuador apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

As mentioned before, regardless of the nationality of the data processor or the place where the data processing takes place, the LOPDP will be applicable when the data owner resides in Ecuador and the processing activities are related to:

- (a) goods or services offered to the owner, whether or not such goods or services are free, or
- (b) monitoring of their behavior, if it takes place in Ecuador.

In terms of requirements, foreign companies covered by this regulation must appoint a special proxy in Ecuador with sufficient powers to act in administrative or judicial proceedings related to data protection. This appointment must be registered before the Superintendence. This obligation may be exempted if the processing is occasional, does not involve sensitive data on a large scale and does not represent a high risk to the rights of data subjects. In all other cases, the foreign company must have a local representative to serve as a liaison with the Ecuadorian authority.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Ecuador?

The LOPDP defines ‘personal data’ in a broad manner, in line with international standards, as ‘any information that identifies or makes identifiable a natural person, directly or indirectly’. This includes basic data such as name, ID number, address, e-mail address, telephone number, as well as indirect identifying data (eg, a unique device identifier or a combination of data that makes it possible to recognize someone).

It should be noted that the law protects only the data of natural persons. Data of legal entities are not considered ‘personal data’ under the LOPDP. Also, the definition includes data in electronic formats as well as data in paper or other media. Typical examples of personal data include: contact information, date of birth, government identifiers, employment or financial data of an individual. All of these, by identifying an individual, fall into the legal category of personal data and are under the protection of the Ecuadorian privacy law.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Generally, ‘sensitive data’ in Ecuador is treated by the Constitution as personal data that reveals racial, ethnic, or religious origin, political positions, and trade union membership, and data concerning a person’s health, sexual life or any other personal data that may cause discrimination to data owners in their lifetime.

The LOPDP distinguishes:

- (a) **Sensitive data:** This is data related to ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial past, immigration status, sexual orientation, health, biometric data, genetic data, and data the improper treatment of which may give rise to discrimination. Its processing is generally forbidden. Exemptions exist, such as the explicit consent of the subject, the data having become public, cases of public interest or where a court order has been made.
- (b) **Personal data of deceased persons:** A deceased person’s successors can request the controller for the right to access, rectify, update, or erase the personal data of the deceased.
- (c) **Credit data:** Processing credit data will be legitimate when it is obtained from publicly accessible sources or from information provided by the creditor. Such data may be used only for analysis purposes and cannot be communicated or disseminated, nor have any secondary purpose. Credit data cannot be processed after five years have elapsed since the debt first became enforceable. Data subjects are entitled to access their credit data at any time and free of charge.
- (d) **Health data:** The National Health System is allowed to collect and process this sensitive data and must guarantee its confidentiality. Consent will not be required in cases of public interest in the field of health. Wherever possible, health data that is processed must be previously anonymized or pseudonymized.
- (e) **Children:** Minors under the age of 15 need their parent or legal representative to provide consent and exercise their rights; teenagers aged 15 and older can grant consent and exercise their rights directly. See further question 7.9.

As a general rule, the processing of such data is prohibited, except in the following cases:

- (i) The data subject, or their parent or legal representative in the cases of children, has given explicit consent for the processing of their personal data, with clearly specified purposes;
- (ii) The processing is necessary for the fulfillment of obligations and the exercise of specific rights of the controller or the data subject in the field of labor law, social security, and health;
- (iii) The processing is necessary to protect the vital interests of the data subject or another person, when the data subject is physically or legally unable to give consent;
- (iv) The processing refers to personal data that the data subject has manifestly made public;
- (v) The processing is carried out by judicial order;
- (vi) The processing is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes, provided it is proportionate, respects the essence of the right to data protection, and includes appropriate safeguards; or
- (vii) The processing of health data is subject to the conditions established by the LOPDP.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The LOPDP excludes from its scope of application truly anonymized data, ie, data that does not allow the identification of a person. Anonymized personal data are not considered personal data and, therefore, the law does not apply to them, as long as the anonymization prevents the identification of the owner. If at some point the data ceases to be anonymized and becomes identifiable again, it again falls under the protection of the LOPDP. In summary, total anonymization allows the handling of information without legal restrictions, but it must be effective; if there is a reasonable possibility of re-identification, the legal protection subsists.

As for pseudonymization, the law recognizes it as a security technique, but does not exempt from compliance with the regulations. ‘Pseudonymization’ means replacing identifying attributes with codes or aliases, so that the real identity can only be obtained through additional separate information. Pseudonymized data is still personal data, as it can still be re-identified, although its use is encouraged as a good practice to reduce risks.

Finally, terms such as ‘de-identified’ or ‘disassociated’ in the regulations often refer to these forms of anonymization. If the de-identification is irreversible, it is equivalent to anonymizing and the data remain outside the legal framework. If it is reversible by means of keys, it is equivalent to pseudonymizing, which is still regulated.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies, being data controllers, have several obligations under the LOPDP to ensure proper management of personal data. They must:

- (a) comply with the guiding principles of the law, such as:
 - (i) transparency (informing data subjects about the use of their data),
 - (ii) purpose (using data only for legitimate purposes),
 - (iii) minimization (collecting only what is necessary) and
 - (iv) security. This implies not keeping data longer than required, not using it in ways incompatible with the initial purpose without motivation, and ensuring the accuracy of the information.

- (b) provide clear privacy notices, including information on:
 - (i) the identity of the data controller,
 - (ii) purposes of the processing,
 - (iii) legal basis,
 - (iv) storage period,
 - (v) recipients and
 - (vi) rights of the holder;
- (c) provide mechanisms for individuals to exercise their rights and respond within the established deadlines. Unjustified refusal or failure to respond may constitute an infringement;
- (d) in terms of security, adopt technical and organizational measures to prevent unauthorized access or leaks;
- (e) notify security breaches,
- (f) sign appropriate contracts with third parties that process data,
- (g) keep an updated register of processing activities;
- (h) appoint a data protection officer ('DPO') when mandated by Law;
- (i) train their staff in data protection; and
- (j) foster an organizational culture aligned with the regulations.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

The LOPDP distinguishes between 'controller' and 'processor'. The controller is the one who decides on the purpose and means of the processing of personal data, while the processor is the one who processes them on the instructions of the controller, usually a service provider. For example, if a company hires an agency to send advertising mailings, the company is the controller and the agency is the processor. This distinction is key because it defines specific obligations in data processing.

The controller must ensure compliance with the law, have a legal basis for the processing, inform the data subjects, protect their rights and choose processors that offer adequate safeguards.

The processor, for its part, must act according to the instructions of the controller, not use the data for its own purposes and sign a contract setting out its confidentiality and security obligations.

In case of non-compliance, both can be sanctioned: the data controller if it did not adequately implement the law and the data processor if it acted outside the agreed conditions.

Companies must correctly identify their role in each processing operation in order to know their obligations.

4.3 **Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

The LOPDP requires that any processing of personal data must have a lawful basis established by law. Processing is only lawful if it falls within the recognized legal bases:

- (a) **Consent of the data owner:** this is the most common lawful basis. It must be free, specific, informed and unequivocal, with the possibility of being revoked at any time;
- (b) **Legal obligation**, when the processing is required by a regulation, or **judicial order**, when a judge so orders;
- (c) **Public interest or exercise of public powers**, applicable to state institutions;

- (d) **Contractual relationship**, ie, when the data are necessary for the execution of a contract with the owner;
- (e) **Vital interests**, ie, in situations where the processing is indispensable to protect the life or health of a person;
- (f) **Data is from publicly accessible sources**, provided that their purpose is respected; and
- (g) **Legitimate interest of the data controller or a third party**, which requires assessing that the rights of the holder do not prevail. In such a case, the holder retains the right of opposition, allowing them to challenge such processing.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

When a company processes personal data for advertising purposes, it must clearly inform the owner by means of a privacy notice. This notice must:

- (a) include the identity and contact details of the data controller, as well as those of the data protection officer, if any;
- (b) specify the purposes of the processing, clearly indicating whether the data will be used for advertising purposes;
- (c) specify the legal basis justifying the processing;
- (d) detail who processes the data, with whom it is shared and
- (e) set out what rights the user has, ensuring transparency and control over their personal data in the advertising context.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) **Right to the protection of personal data:** This right is recognized in the Constitution of the Republic of Ecuador;
- (b) **Right of access:** The holder may request information about the processing of their personal data, including a copy of the data and details about its use and possible transfers to third parties;
- (c) **Right to rectify and update:** This allows correction of inaccurate data or completion of incomplete information in the databases of the data controller;
- (d) **Right of deletion (cancellation):** The holder may request the deletion of their data when they consider that it is no longer necessary for the purpose for which it was collected or when they have withdrawn their consent;
- (e) **Right of opposition and revocation of consent:** The owner has the right to oppose the processing of their data for certain purposes, especially in marketing, as well as to withdraw consent when this has been the legal basis for the processing;
- (f) **Right of portability:** This allows the owner to request their data in a structured and commonly used format or to request its transfer to another data controller; and
- (g) **Right not to be subject to automated decisions with significant effects:** This guarantees that the holder may request information, challenge decisions or demand human intervention in cases where algorithms or profiling may significantly affect them.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Sending messages or calls for commercial purposes without express consent constitutes an infringement of the Organic Telecommunications Law. This obliges companies to obtain authorization before sending advertising, in order to obtain consent. In addition, when dealing with minors or special categories of data, even stricter consent is required.

Each communication must include clear and free opt-out mechanisms. Companies must register and respect these opt-outs in their databases and train their personnel to process them correctly. In addition, the Superintendence can sanction non-consensual advertising practices, so these measures are not only recommended, but mandatory for regulatory compliance.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The LOPDP requires that when a company hires a third party to process personal data for advertising purposes, the third party must guarantee the protection of the data. If the third party acts on behalf of the controller, it is a processor and this is not considered a transfer of data, provided that there is a contract with clear clauses on use, confidentiality and security. Such a contract must specify that the processor may only process the data according to the instructions of the controller, without sharing or using it for other purposes, and must implement appropriate security measures and delete or return the data at the end of the service. On the other hand, if the third party uses the data for its own purposes, a data transfer is configured, which requires a valid legal basis, usually the consent of the owner, with exceptions. Even with consent, the recipient must respect the agreed purpose and implement adequate protection measures.

The use of technology providers in advertising implies an evaluation of compliance by the data controller. The company must select suppliers that offer adequate data protection guarantees and sign confidentiality agreements with all parties involved. In case of non-compliance, both the supplier and the contracting company may be sanctioned, especially if there was negligence in supervision.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

- (a) **When a company shares personal data with a third party data processor**, it must establish a contract with specific clauses to guarantee data protection. This contract must include:
 - (i) precise instructions on the processing of the data, restricting its use to authorized purposes, in addition to requiring the confidentiality of the information;
 - (ii) the applicable security measures;
 - (iii) the destination of the data at the end of the contractual relationship (return or certified deletion); and
 - (iv) the obligation of the processor to cooperate with the controller in complying with the regulations.

In addition, if the processor wishes to hire sub-processors, it must have the express authorization of the data controller. The processor is also required to immediately inform the controller in case of security breaches.

- (b) **When a company receives personal data from a third party**, it is advisable to formalize a contract in which the provider guarantees that it obtained the data legitimately and in compliance with the LOPDP. Although, in these cases, both parties usually act as independent controllers, the receiving company could be affected if the provider obtained the data without consent or unlawfully. For this reason, the provider must be required to prove that it has a valid legal basis for the transfer and assume liability in the event of misrepresentation. In international transfers, specific clauses should be included that oblige the foreign recipient to comply with the LOPDP and submit to the Ecuadorian authority in case of dispute.

It is essential to contractually document the responsibilities of each party. It is recommended to include:

- (i) audit clauses so that the person in charge can verify the provider's compliance;
- (ii) incident notification to report security breaches; and
- (iii) contractual termination conditions in the event of serious breaches.

It is also advisable for the processor to assist in impact assessments or prior consultations with the authority if the type of processing requires it. In summary, the company must protect itself contractually both when sharing and receiving data, ensuring that all parties comply with the LOPDP. This is not only an obligation set out in the Regulation, but a key strategy to avoid shared responsibilities and ensure compliance.

6.3 **What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?**

The LOPDP adopts the principle of proactive responsibility (accountability), which implies that companies must act with due diligence in the management of personal data, anticipating risks and demonstrating compliance.

The controller and the processor can voluntarily adhere to codes of conduct, certification, seals or standard clauses, without this constituting an exemption from the responsibility to comply with the provisions of this law, its regulations and directives from the Superintendence.

One example of a good practice mentioned by the Law is the voluntary appointment of a DPO, even when not legally required. This measure helps demonstrate the organization's commitment to proactive responsibility. The regulation also encourages designating a deputy officer to ensure uninterrupted oversight in case of absence or impediment of the primary officer.

The POPDP requires controllers to apply to apply technical, legal, administrative, and organizational measures that ensure, and can demonstrate, that data processing complies with the applicable regulations. These measures must be analyzed within the nature, scope, purpose, and risks of the processing activity and must be regularly reviewed and updated. However, the POPDP does not establish or define a specific set of required actions. As a result, although proactive responsibility is framed as mandatory, its concrete implementation often relies on other provisions of the POPDP or its Regulation that expressly set out specific, enforceable duties for data controllers and processors, which have been discussed previously.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Advertising calls or messages are expressly prohibited without prior authorization. Consent must be informed, clear and freely given, ensuring that the user knows the purpose of the processing of their data and has the possibility to withdraw it at any time. In addition, companies must adequately inform the user before obtaining consent for these communications.

If direct marketing is directed to existing customers, the principle of legitimate interest of the data controller may apply. In addition, companies must comply with key data protection principles, such as minimization, purpose and security. They must not collect data in excess or use it for purposes other than those reported without a legal basis for doing so.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies, such as cookies, pixels, web beacons and SDKs in mobile applications, involve the processing of personal data when they collect information linked to an identifiable user. Although the LOPDP does not have a specific section to regulate them, general data protection principles apply, including transparency, lawfulness, minimization and security. The company using these technologies must clearly define their purpose and have a valid legal basis for their implementation. In most cases, the legal basis will be the user's informed consent when cookies or SDKs are not strictly necessary for the operation of the service .

The principle of minimization requires that only data strictly necessary for the stated purpose are collected. If cookies or SDKs are used to personalize advertising, analyze behavior or track user activity, the user must be clearly informed about what data is being collected and for what purpose. It is also necessary to ensure that the user has the option to accept or reject these technologies through accessible privacy settings. Although there are no specific regulations on cookie banners, the recommended practice is to implement consent systems that allow the user to manage their preferences.

In terms of the security of the data collected, companies must take measures to prevent unauthorized access or misuse. They must also establish retention limits, ensuring that the identifiers collected are not stored longer than necessary. In the case of data transfers to third parties, such as advertising platforms or analytics tools, adequate safeguards must be in place and recipients must be verified for compliance with applicable data protection regulations.

In short, the use of tracking technologies must comply with the LOPDP, ensuring that users have control over their privacy and that the data is treated in a transparent and secure manner.

7.3 How are loyalty programs and promotions regulated under privacy law?

Equivalent to the previous response.

7.4 How is social media and influencer marketing regulated under privacy law?

Equivalent to the previous response.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Equivalent to the previous response.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Equivalent to the previous response.

7.7 How is location-based advertising regulated under privacy law?

Equivalent to the previous response.

7.8 How are data brokers defined and regulated under privacy law?

Data intermediaries operate as controllers or processors, depending on their degree of control over the data. In this case, they must comply with all the obligations established in the LOPDP, including the lawful collection of data, transparency in processing and guaranteeing the exercise of rights by data subjects. The intermediary must have a lawful basis for obtaining and transferring personal data. In most cases, if the purpose is to market the data to third parties, the express consent of the data subject is required.

In addition, the LOPDP requires the registration of databases before the National Registry of Personal Data Protection. This mechanism allows the authority to supervise the activity of these operators, reducing the risks of misuse of information. An intermediary that does not register its databases could incur an infraction. Severe penalties are also established for the unauthorized sale of data, which can reach up to 1% of the offender's turnover. Additionally, the Constitution guarantees any person the right to access personal data stored by public or private entities. Accordingly, intermediaries must be prepared to respond to requests for access and, where appropriate, delete the owner's information, subject to legal exceptions.

In certain sectors, such as the credit market, regulation is even stricter. Credit bureaus and credit registries are subject to both the LOPDP and specific regulations, and must allow cardholders to access, rectify and delete inaccurate information about their financial history.

7.9 How is advertising to children and minors regulated under privacy law?

Ecuador's data protection law grants special protection to the personal data of children and adolescents, categorizing them as sensitive data. See question 3.2.

Children and adolescents also have the right not to be subject to decisions based solely or partially on automated processing, unless there is express authorization from the minor (if aged 15 or older) or from their legal representative, or if the processing is carried out to safeguard an essential public interest.

Minors aged 15 or older may provide explicit consent for the processing of their personal data, as part of the progressive exercise of their rights, provided the purposes are clearly explained. Otherwise, consent must be obtained through their legal representatives, parents or guardians.

Lastly, in the event of the death of a minor, rights such as access, rectification, update, or deletion of personal data may be exercised by their last legal representative, and the law requires specific safeguards to protect the fundamental rights of the data subject in such cases.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Every data subject has the right not to be subject to a decision based solely on automated processing, including profiling, when such decision produces legal effects or significantly affects their rights. However, in the advertising context, this provision is not automatically triggered, since most decisions based on algorithms do not generate legal consequences or a serious impact on the rights of the holder (the right does not apply when the decision does not entail relevant impacts or verifiable risks).

However, the use of automated decisions in advertising is subject to the duty of transparency. The data controller is obliged to inform data subjects if automated assessments or decisions, including profiling, are made on their personal data. Thus, any company that uses AI or algorithms for advertising purposes must communicate this clearly, for example, through its privacy policy or at the time of collecting the data. This communication is essential, as it triggers the right of the data subject to object to profiling for marketing purposes.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

As a general principle, the international transfer or communication of personal data is allowed when the recipient country ensures an adequate level of protection, consistent with internationally recognized standards, as determined by the criteria established in the Regulation. The Superintendence may implement ex post control mechanisms to monitor compliance.

To declare that a country provides an adequate level of protection, the Superintendence must issue a resolution identifying such jurisdictions. As of now, no official list of countries has been published. If the destination country is deemed adequate, no prior authorization is required for the transfer.

When data is to be transferred to a country not recognized as adequate, the controller or processor must offer sufficient guarantees to protect the rights of the data subject. These include:

- (a) ensuring compliance with data protection principles and obligations at a level equal to or higher than those under Ecuadorian law;
- (b) guaranteeing the effective enforcement of data subject rights through accessible administrative or judicial remedies; and
- (c) securing the right to full reparation, where applicable.

Additionally, the law allows for exceptional transfers even in the absence of adequate protection or guarantees, in the following specific cases such as:

- (i) institutional competence fulfillment;
- (ii) explicit informed consent of the data subject;
- (iii) compliance with legal or regulatory obligations;
- (iv) performance of a contract or pre-contractual measures at the request of the data subject;
- (v) public interest;

- (vi) international judicial cooperation;
- (vii) investigation of infringements;
- (viii) international cooperation commitments;
- (ix) banking and financial operations;
- (x) legal claims or defense; and
- (xi) protection of vital interests where consent cannot be obtained.

In practice, while there is no outright ban on transfers to specific countries, transfers to jurisdictions without an adequacy declaration require case-by-case safeguards or must fall under one of the explicitly allowed exceptions.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Companies should be aware of contractual considerations or legal confidentiality, such as banking confidentiality. All this is encompassed in the notion of ‘responsible transfer’, not only to comply with the LOPDP, but to ensure in practice that the holder’s privacy suffers the least possible detriment.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Ecuador? Are there minimum standards? Does this differ by sector or size of the entity?

The LOPDP establishes that all data controllers and processors must implement adequate security measures to protect personal data against unauthorized access, alteration or misuse. No specific technical standard is required, but the principle of proportionality is established, which means that the levels of protection must be adjusted to the sensitivity and volume of the data processed. Technical, organizational, physical and legal measures must be taken to ensure security, alongside actions to prevent and mitigate risks. Although the Regulation does not set specific technical parameters, it is foreseeable that the authority will recommend practices of a sensitive nature.

Security measures vary according to the regulated sector. For example, in the financial sector, the Banks Superintendence establishes specific rules for the classification and protection of information. In telecommunications, ARCOTEL imposes confidentiality requirements in data handling, and the LOPDP obliges all state entities to have a data protection officer, ensuring an internal structure of compliance and security, reinforced by a mandatory Resolution of the Superintendence.

The General Regulation foresees the issuance of specific guidelines by the Superintendence, which could include more detailed sectoral and technical standards. In addition, the LOPDP mentions the possibility of data protection certifications and seals, suggesting that large companies may adopt international standards such as ISO 27701 to demonstrate compliance, although the latter are not mandatory.

9.2 How are personal data breaches regulated in Ecuador? What are the requirements for notification and response?

In Ecuador, personal data breaches are subject to mandatory notification requirements. When a data breach occurs, the controller must notify the Superintendent and ARCOTEL as soon as possible, and no later than five days after becoming aware of the incident, unless the breach is unlikely to pose a risk to the rights and freedoms of individuals. If the notification is made after this deadline, the controller must explain the reasons for the delay.

Meanwhile, the processor, for its part, must notify the controller of any breach without undue delay, and no later than two days from the moment it becomes aware of the incident.

These obligations are designed to ensure timely containment of risks and enable prompt action to protect data subjects. Failure to comply with these deadlines may result in administrative sanctions and liability under Ecuador's data protection framework.

The notification must include:

- (a) the nature of the incident,
- (b) the type and volume of data compromised,
- (c) the approximate number of data subjects affected,
- (d) the possible consequences,
- (e) the measures taken or planned to mitigate the damage, and
- (f) a contact for follow-up.

If the incident represents a high risk to the rights of data subjects, the affected persons must also be informed directly, without undue delay.

Following notification, the Superintendence may issue additional instructions, initiate an investigation or even impose sanctions if it identifies negligence. The company, in addition to complying with the notification, must mitigate the damage, remedy the vulnerability and review its security measures to prevent future incidents, in accordance with the principle of proactive responsibility.

Compliance with this obligation is essential. Failure to report a violation is considered an infraction, which may be classified as minor or serious depending on the case and may result in fines and penalties.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

There is an administrative sanctioning regime based on the seriousness of the infringement and the type of infringer. Infringements are classified as minor and serious, and fines for legal entities range from 0.1% to 1.0% of annual turnover. Minor infractions are sanctioned with fines between 0.1% and 0.7% of annual turnover, while those for serious infractions range from 0.7% to 1%. For public officials, fines are personal: from 1 to 10 Basic Salaries for minor infractions and 10 to 20 Basic Salaries for serious ones. In addition, the Superintendence may impose corrective measures, such as suspension of data processing, elimination of illegal databases or mandatory implementation of security measures. There is also the possibility of public reprimands or reputational measures.

The sanction imposed is determined according to proportionality criteria, including intentionality, recidivism, number of people affected and the seriousness of the damage. In cases of repeated or serious infringement, the authority may impose the maximum sanction and, in the case of public entities, refer reports for disciplinary sanction or dismissal. No custodial penalties are contemplated, since the sanctions are administrative in nature, without prejudice to possible civil actions for damages.

10.2 Do consumers have a private right of action? What remedies are available to them?

The LOPDP, together with the Constitution of Ecuador, recognizes several ways in which data subjects may protect their rights in case of violation. The action of *habeas data* allows access to personal data contained in public or private files in order to know its purpose, origin, recipients and request its update, correction or deletion. This judicial guarantee may be used when a responsible party refuses to comply with the holder's rights.

Data subjects may file civil actions for tort liability under the Civil Code to claim compensation for material or moral damages arising from the unlawful processing of personal data. This possibility is supported by the Constitution itself, which expressly establishes the right to sue for damages. In addition, administrative complaints may be filed with the Superintendence, which is empowered to impose sanctions, corrective measures and order the reparation of rights.

Where a group of consumers have been affected, it is possible to initiate actions for the protection of collective or diffuse rights in accordance with the Constitution, even when the LOPDP does not expressly regulate them. Such actions may be brought by consumer organizations or the Ombudsman's Office. Remedies include not only the correction of improper processing, but also the right to full reparation, which may include financial compensation, data deletion, guarantees of non-repetition and restoration of moral damages.

Thus, the regulatory framework provides judicial, civil and administrative remedies to ensure the effective protection of personal data.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Since the entry into force of the LOPDP was only in May 2023 and the Superintendent appointed in 2024, the regulatory framework in Ecuador is still in a phase of progressive implementation. The Superintendence, as the authority in charge, has begun to hear complaints, issue resolutions and initiate ex officio investigations. Although there have been no sanctioning cases so far, there is already an active orientation towards the control of data processing, especially in advertising contexts.

In the meantime, many companies have begun to adjust their data processing practices by making internal audits, obtaining consents and adapting their communication channels. The evolution of this first stage shows a combination of prevention, regulatory guidance and control which will set the standard for compliance in the coming years. The Superintendence issues annual Resolutions indicating the planning of the line of work; and has already issued secondary regulations such as the Technical Guide for the Registration of Special Proxies and the Regulation for filing Complaints and Requests.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Ecuador?

Traditionally, the informal use of personal data and the low awareness of privacy generated little social demand. However, in recent years, public attention to the issue has increased, forcing the Superintendence to adopt a progressive approach.

This is in addition to the country's ethnic-linguistic diversity and the constitutional incorporation of the principle of Good Living, which would position data protection as a guarantee of dignity and privacy.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

The privacy and advertising environment in Ecuador is advancing rapidly, driven by the full implementation of the LOPDP and the development of new guidelines by the Superintendence. Companies will also need to adapt to possible reforms or additional restrictions on sensitive issues such as the processing of minors' data, digital marketing without consent and the use of identity solutions. In this dynamic context, a corporate culture of continuous compliance, regulatory monitoring and proactive adaptation is required.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

It is essential for companies to understand that personal data protection is not a one-time compliance, but a continuous process that requires planning, monitoring and adaptation. The LOPDP imposes obligations that, while they may seem complex at first, can become a competitive advantage when managed strategically. Adopting a proactive compliance approach allows companies to anticipate sanctions, reduce operational risks and strengthen customer relationships through trust.

In this context, it is important to choose the most appropriate legal strategy, especially because the Ecuadorian regulatory framework on privacy matters is undergoing a complete evolution. The issuance of new regulations, technical guides and interpretative criteria by the supervisory authority means that requirements may change in the short term. Therefore, having specialized legal advice not only facilitates the initial implementation of the LOPDP, but also guarantees an updated accompaniment to adapt to new obligations as they arise.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, Ecuador has experienced significant advances in the field of personal data protection. The implementation of the LOPDP, approved in 2021, has been central to this process, as it was the genesis of the evolution of this field. In November 2023, the General Regulation that develops this law was approved, establishing the necessary aspects for the Superintendence to take over as the authority in charge of supervising and controlling the processing of data in the country. The Superintendence has been organically structuring its team and has already issued some important resolutions, such as Resolution SPDP-SPDP-2024-0002-R, which establishes the obligation of foreign data controllers and processors to appoint a special representative in Ecuador, and directives such as the procedure for attending public consultations. Also, its first official investigation has been initiated, but is confidential and its resolution is still pending.

Globalization and the massive exchange of information have highlighted the importance of safeguarding citizens' privacy, motivating the country to strengthen its legal framework in this area.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

One of the biggest challenges is the need to adapt operationally to a legal framework still under consolidation. Many organizations, especially small and medium-sized ones, lack internal structures to comply with principles such as lawfulness, minimization or proactive responsibility, which will require investment in policies, training and technology. Added to this is the uncertainty derived from the absence of jurisprudence or uniform criteria by the authority, which generates doubts about how to apply legal bases such as consent or legitimate interest, and how to address practices such as profiling, digital marketing or the use of artificial intelligence; this increases the need for specialized advice to avoid future sanctions.

12.3 What do you envision the privacy landscape will look like in five years?

The privacy landscape in Ecuador is projected as a more consolidated and demanding regulatory environment, with an effective application of the LOPDP. Although no firm sanctioning resolutions have been issued at present, it is foreseeable that in five years' time the Superintendence will have issued a relevant set of decisions that will constitute administrative jurisprudence and provide guidance to both legal operators and data controllers. The trend is for the Ecuadorian authority to follow the line of its international peers—strongly sanctioning the most obvious violations such as lack of consent and serious security breaches—and this evolution will make it possible to delimit more clearly the compliance standards, the substantive obligations and the proportionality criteria applicable to each sector.

In parallel, greater institutional and cultural maturity in privacy management is expected. Companies will incorporate proactive compliance practices into their structures, appoint internal data protection officers and adopt impact assessment tools, especially in advertising, financial and digital environments. Citizens will also become more aware of their rights and be more active in their defense, which will drive a stronger role for the authority.

EGYPT

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Egypt.

Privacy in Egypt is primarily regulated under the Egyptian Constitution and the Personal Data Protection Law. The law governs the collection, processing, transfer, and storage of personal data and applies to both Egyptian and foreign entities handling personal data in Egypt. Enforcement falls under the Personal Data Protection Center, which is responsible for implementing regulatory measures and issuing necessary permits and licenses.

1.2 What are the primary laws regulating privacy in Egypt? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Egyptian privacy law is governed by:

- (a) The Egyptian Constitution (2014)—Article 57 guarantees privacy rights, stating that private communications cannot be monitored or seized without judicial oversight.
- (b) Law No 151 of 2020 ('Personal Data Protection Law')—This establishes rules for processing, storing, and transferring personal data and requires explicit consent for data collection.
- (c) Law No 175 of 2018 ('Anti-Cybercrime Law')—This criminalizes unauthorized access to private data and personal communications.
- (d) Law No 180 of 2018 ('Media Regulation Law')—This regulates digital content and social media with over 5,000 followers.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays a minimal role in privacy protection in Egypt. However, companies engaging in advertising must ensure compliance with the Personal Data Protection Law when collecting or processing personal data, particularly regarding user consent and targeted marketing.

1.4 How is privacy law enforced in Egypt? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Personal Data Protection Center is the primary regulatory body, responsible for:

- (a) issuing permits for data processing activities;
- (b) investigating data breaches and privacy violations;
- (c) enforcing penalties for non-compliance; and
- (d) overseeing cross-border data transfers.

The Egyptian Economic Courts have jurisdiction over violations of the Personal Data Protection Law.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Egypt?

The law applies to all natural and legal persons processing personal data electronically in Egypt. It also covers entities outside Egypt if their processing activities involve Egyptian citizens or residents.

2.2 Does privacy law in Egypt apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. Foreign companies must comply with Egyptian privacy law if they process data related to Egyptian citizens or residents. They must also appoint a local representative in Egypt.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Egypt?

‘Personal data’ includes any information that directly or indirectly identifies a natural person, such as names, ID numbers, biometric data, financial records, or online identifiers.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive data’ includes information about health, genetics, biometrics, religious beliefs, political opinions, criminal records, and children. Such data can only be processed with explicit consent or legal authorization.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The law does not specifically address pseudonymized or de-identified data. However, if data can be re-identified, it is subject to the Personal Data Protection Law.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must:

- (a) obtain explicit consent before processing personal data;
- (b) implement security measures to protect data;
- (c) notify the regulator of breaches within 72 hours; and
- (d) appoint a data protection officer (‘DPO’) if required.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. Companies can act as data controllers or data processors, with different obligations related to data security, processing agreements, and compliance monitoring.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes. Processing must be based on:

- (a) consent of the data subject;
- (b) legal obligations;
- (c) performance of a contract; and
- (d) public interest.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The following information should be included:

- (a) purpose of data collection;
- (b) legal basis for processing;
- (c) data retention period; and
- (d) rights of the data subject.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the following rights:

- (a) right of access to and correction of their data;
- (b) right to withdraw consent;
- (c) right to object to processing; and
- (d) right to request deletion or restriction of processing.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies must obtain prior opt-in consent for direct marketing via electronic means (ie, email, SMS, push notifications).

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Egyptian privacy law does not yet provide explicit guidance on advertising vendors such as DSPs or data providers. However, general obligations apply. Controllers must ensure that vendors implement appropriate data protection measures, and processing must be governed by written contracts clearly outlining responsibilities.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Contracts with third parties must include clauses on data confidentiality, security obligations, breach notification requirements, and restrictions on cross-border data transfers unless prior regulatory approval has been granted.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies are expected to carry out due diligence when engaging vendors, including security reviews and regulatory approvals where needed. Data protection impact assessments are strongly recommended for high-risk activities such as profiling, automated decision-making, and targeted advertising.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Companies must obtain prior consent before sending marketing communications, and must provide an opt-out mechanism.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

No specific regulations exist on cookies and tracking technologies, but explicit consent is recommended.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs must be designed to collect only necessary personal data and must not be used for marketing unless explicit consent is obtained. Transparency around data use, retention, and third-party sharing is essential.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media platforms must comply with privacy laws, and accounts with over 5,000 followers are subject to additional media regulations.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising requires opt-in consent, especially where profiling is involved. Contextual advertising that does not rely on personal data may not require consent but must still comply with general transparency obligations.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

These are not specifically regulated under Egyptian law but would fall under broader obligations related to data minimization, purpose limitation, and security safeguards.

7.7 How is location-based advertising regulated under privacy law?

Use of geolocation data for advertising requires prior consent. Users must be informed of how their location data is used and provided with a clear option to opt out.

7.8 How are data brokers defined and regulated under privacy law?

There is no specific definition or regulation of data brokers under current law. However, any entity collecting and selling personal data must comply with the law's consent, purpose limitation, and data security requirements.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising directed at children is not yet comprehensively regulated under privacy law, but sensitive data involving minors (e.g., online behavior) requires parental consent.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Automated decision-making and profiling using AI must be transparent and based on valid consent. Where such technologies materially impact individuals (eg, pricing or access decisions), companies should provide mechanisms for user intervention or review.

7.11 Are there other specific advertising practices that you wish to discuss?

Advertisers using biometric technologies (eg, facial recognition) must be especially cautious, as this would qualify as sensitive data and require both regulatory authorization and explicit consent.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes. Transfers are only allowed if the receiving country offers equivalent data protection. Exceptions exist for:

- (a) legal necessity;
- (b) contractual obligations; and
- (c) medical emergencies.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

For transfers involving privileged or sensitive data (such as legal, medical, or national security matters), heightened security and potentially regulator consultation are recommended.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Egypt? Are there minimum standards? Does this differ by sector or size of the entity?

Companies must implement technical and organizational measures to prevent unauthorized access, data loss, or breaches.

9.2 How are personal data breaches regulated in Egypt? What are the requirements for notification and response?

Companies must notify the Personal Data Protection Center within 72 hours of detecting a breach and must inform affected individuals within three days.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Fines range from EGP 100,000 to EGP 5 million depending on the violation. Severe breaches may lead to imprisonment.

10.2 Do consumers have a private right of action? What remedies are available to them?

No. Consumers must file complaints with the regulator, who decides on enforcement actions.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement is still evolving. However, authorities have recently increased scrutiny on telecoms and banks for data retention and marketing breaches. No notable advertising-related court decisions have been published yet.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Egypt?

Egypt places national security interests above individual privacy, with broad government access to personal data.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) The issuance of executive regulations for the Personal Data Protection Law; and
- (b) Greater enforcement actions by the regulator.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Organizations are advised to monitor the forthcoming executive regulations under the Personal Data Protection Law and to prepare for audits by the Personal Data Protection Center, especially in advertising and digital marketing sectors.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The Personal Data Protection Law (2020) was the most significant development, aligning Egypt with global data protection standards.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

- (a) Unclear enforcement mechanisms; and
- (b) Compliance costs for data processing and security requirements.

12.3 What do you envision the privacy landscape will look like in five years?

- (a) Increased regulatory enforcement;
- (b) Potential alignment with GDPR-style frameworks; and
- (c) Stronger penalties for non-compliance.

EL SALVADOR

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in El Salvador.

In November 2024, the Legislative Assembly approved the Law for the Protection of Personal Data. This was published in the Official Gazette on November 15, 2024 and became effective on November 23, 2024.

Its purpose is to establish regulations for the protection of personal data, determining the requirements for legitimate and informed processing, and regulating the collection, use, processing, and storage of personal data to guarantee individuals' right to privacy.

1.2 What are the primary laws regulating privacy in El Salvador? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy is primarily regulated in the following Laws:

- (a) Constitution of El Salvador;
- (b) Special Law against Computer and Related Crimes; and
- (c) Law on Access to Public Information;
- (d) Law on the Regulation of Information Services on People's Credit History;
- (e) Medicines Law;
- (f) Consumer Protection Law;
- (g) Law for the Protection of Personal Data;
- (h) Cybersecurity and Information Security Law; and
- (i) Banking Law; and
- (j) Law on the Supervision and Regulation of the Financial System.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In El Salvador, the new Law for the Protection of Personal Data addresses self-regulation, although not in regard to advertisements. Self-regulation means that each person has rights to obtain all information about themselves found in all databases or physical records. Also, if the personal data was provided for specific means which are no longer needed, they have the right to request the cancellation of their personal data.

However, the entities in charge of regulating privacy vary, depending on the matter in hand; for instance, the Superintendence of the Financial System and Consumer Advocacy is the regulatory entity in the case of banks.

1.4 How is privacy law enforced in El Salvador? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Law for the Protection of Personal Data is enforced through the State Cybersecurity Agency whose remit includes:

- (a) to control, inspect, and supervise the institutions obligated under the scope of application of the Law for the Protection of Personal Data;
- (b) to exercise the power to impose sanctions in matters of personal data protection and in accordance with the terms established by the Law for the Protection of Personal Data;

- (c) to issue, modify, or annul provisional measures as provided by the Law of Administrative Procedures;
- (d) to guarantee the effective protection of personal data in accordance with the powers granted by the Law for the Protection of Personal Data;
- (e) to promote awareness programs on this law directed at the obligated parties and the public, with emphasis on raising public awareness and understanding of the risks, rules, safeguards, and rights related to personal data processing, with special focus on children, adolescents, and older adults;
- (f) to resolve disputes that arise between data subjects, controllers, and processors regarding the classification and declassification of sensitive personal data;
- (g) to provide technical support, when required, to data controllers in the development and execution of their personal data protection programs;
- (h) to co-operate, particularly through information-sharing—though not personal or sensitive data—with other supervisory authorities in the exercise of their duties and provide mutual assistance to ensure consistency in the implementation and enforcement of the Law for the Protection of Personal Data;
- (i) to establish policies for the handling and maintenance of personal data, as well as the related security and protection measures, seeking the implementation of international best practices whenever applicable;
- (j) to create data protection certification mechanisms and seals and marks for the same purposes, and to authorize third parties to issue certifications on the subject;
- (k) to conduct periodic reviews of the certifications referred to in the previous item, when appropriate;
- (l) to carry out annual audits of the certifications issued;
- (m) to provide training to public and private institutions, as well as their members, on personal data protection and management;
- (n) to issue guidelines for implementation of the Law for the Protection of Personal Data, which must be published on its website, social media, and any other means deemed appropriate;
- (o) to advise and cooperate with obligated entities in complying with the Law for the Protection of Personal Data;
- (p) To recommend contractual clauses that guarantee the protection of personal data in accordance with this law.
- (q) to develop form templates for the exercise of ARCO-POL rights (see question 5.2) and for the revocation of consent by personal data holders;
- (r) to conduct or support scientific or academic research on the application of the Law for the Protection of Personal Data;
- (s) to assist and advise citizens who request guidance on the scope of the Law for the Protection of Personal Data and the legal means available to defend the rights it guarantees;
- (t) to request from public and private entities information related to the background, documents, programs, or other elements concerning the processing of personal data, ensuring the integrity, security, and confidentiality of the provided information and elements;
- (u) to provide appropriate advice to the Executive Branch in its consideration of draft laws that relate, in whole or in part, to the protection of personal data; and
- (v) any other duties assigned by the Law for the Protection of Personal Data, its regulations, or other applicable legal provisions.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in El Salvador?

Privacy law applies to the government, autonomous institutions, municipalities, corporations of mixed economies, individuals and legal persons (public or private).

2.2 Does privacy law in El Salvador apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

No, privacy law in El Salvador does not apply to companies outside the country. However, it does apply to foreign corporations that operate in the country.

A local representative must be appointed only if the foreign company is the recipient of an international transfer of personal data, which will only be permitted if the receiving country or importer of the personal data complies at least with the data protection principles set out by the Law of El Salvador.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in El Salvador?

‘Personal information’ is private information concerning a person, identified or identifiable, relating to their nationality, address, heritage, email, telephone number and so on.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive personal information’ is information that relates to a person’s creed, religion, ethnic origin, political affiliation or ideologies, union affiliation, sexual preferences, physical and mental health, moral, family situation and other intimate information of a similar nature, or information that could affect the right to honor, to one’s own image, or to personal and family privacy.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The Law for the Protection of Personal Data addresses dissociation and anonymization, calling it an irreversible procedure by which personal data is no longer associated with its owner or, due to its structure, content, or degree of disaggregation, no longer allows identification of the owner.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The Law for the Protection of Personal Data regulates this matter:

- (a) By the Principle of Transparency, the data controller must inform the data subject of all the details of the processing to which their data will be subjected. This information must be provided in a concise, easily accessible manner, and in clear and simple language. The use of lengthy text, technical or legal terminology, and/or fine print is prohibited;
- (b) the data subject must freely express that they agree to share their information with the company, through a declaration or affirmative action;

- (c) the data controller must ensure that they have the security measures in place for its protection, guaranteeing its confidentiality and integrity;
- (d) the data subject has the right to know who holds that information;
- (e) the data subject must be informed beforehand in a clear, express, and unequivocal manner that their data is being stored; therefore, the following must be communicated:
 - (i) purpose or goal of the collection,
 - (ii) the existence of a database,
 - (iii) identity of the data controller, which facilitates contacting the party responsible if necessary,
 - (iv) content of ARCO-POL rights (see question 5.2); and
 - (v) mechanisms of protection and security;
- (f) the company receiving the data must have manuals that specify their operations for the obtaining, use, recording, organization, conservation, dissemination, storage, possession, access, management, and disclosure of personal data; and
- (g) the company receiving the personal data must always guarantee that the data subject can have access to the information, and free of charge.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, banks are the best example of this, since sometimes the Superintendence of the Financial System (controller) requests the banks to provide information on deposits and accounts, as this is information that can only be given to its owners.

A data controller is a natural or legal person, public or private, who manages the database and/or repository, or whoever decides on the purpose and means of processing the personal data they manage or possess.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The data controller must process the personal data in its possession, prioritizing the protection of the interests of the data subjects and refraining from processing or collecting data through fraudulent, unfair, and/or illegal means.

The data controller must comply with any request made by the data subject or their representative free of charge and issue a decision within 20 business days of receipt of the request. Failure to comply with this obligation within the specified period will entitle the data subject to file a complaint with the data delegate to ensure their rights are guaranteed.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The law does not specifically regulate the subject of advertising; but, in general, privacy notices must contain:

- (a) address of the person responsible within the company;
- (b) details of the personal data that will be subject to processing, identifying those that are sensitive;

- (c) legal basis that empowers the responsible party to carry out the processing;
- (d) purposes of the processing for which personal data is obtained;
- (e) mechanisms, means, and procedures to exercise ARCO-POL rights and revoke consent;
- (f) name of the data delegate for the protection of their personal data; and place or means to submit the ARCO-POL request;
- (g) establish means by which the party responsible will communicate changes to the privacy notice;
- (h) contact details of any subcontracted entity for data processing (if applicable); and
- (i) information on the use of cookies.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have ARCO-POL Rights: These are personal and independent rights of Access, Rectification, Cancellation, Opposition, Portability, Oblivion, and Limitation, through which the data subject can exercise control over the processing of their personal data. Also, in the case of advertising, the Law for the Protection of Personal Data states that all individuals must authorize the use of their personal data, so consumers have the right to provide their personal data and/or limit it.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

There is no regulation in this regard, focused on advertising in the Law for the Protection of Personal Data.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

There is no regulation in this regard, focused on advertising in the Law for the Protection of Personal Data.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The processing of personal data by all data controllers may only be carried out for purposes for which the data subject has been informed in advance. When this personal information is transferred to a third party to offer other types of services or for a purpose other than that for which it was collected, the data subject's authorization must be obtained.

The obligations that the data controller must fulfill are:

- (a) limit the processing of personal data to the purpose for which the data subject's consent was issued;
- (b) implement security measures and comply with policies in accordance with the law;
- (c) maintain confidentiality in the processing of personal data; and
- (d) any other obligations assigned by law.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

There is no explicit regulation for this, however all companies must send their clients a form which the clients are obliged to fill out with relevant information in regard to their commercial activities, personal information and company information.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data. It only requires that the privacy notice specifies the use of cookies.

7.3 How are loyalty programs and promotions regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.4 How is social media and influencer marketing regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.7 How is location-based advertising regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.8 How are data brokers defined and regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.9 How is advertising to children and minors regulated under privacy law?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There is no regulation regarding this in the Law for the Protection of Personal Data.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The Law for the Protection of Personal Data stipulates that the transfer of data of any kind to other countries or international organizations is permitted, provided that the receiving or importing country complies with, at a minimum, the personal data principles defined in the Law for the Protection of Personal Data or by international standards on the subject. The guarantees required by El Salvador's law cannot be less.

The person responsible for the transfer of personal data must enter into a contract with the recipient controller, such contract must contain at least the same obligations as those to which the person responsible for the transfer of the data is subject.

In accordance with the Banking Law, companies that form part of a financial conglomerate can share customer databases. Each company that is part of the conglomerate may make economic information regarding their customers available to other financial entities, mostly in regard to their credit background, with the prior authorization of the Superintendence of the Financial System.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Different companies will have different requirements or restrictions regarding the transfer of data, and it is necessary that each company keeps itself informed of its obligations with respect to its customers.

In most cases, data transfer is done by cooperation, and usually in circumstances when there is a resolution issued by a judge, or for use in some judicial case; for example, when database holders are subject to audits or are being investigated for some type of criminal act, and need to exhibit the information contained in databases in the procedure.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in El Salvador? Are there minimum standards? Does this differ by sector or size of the entity?

There is no regulation regarding this in the Law for the Protection of Personal Data.

According to the Special Law against Computer and Related Crimes, anyone who, without authorization, uses personal data through the use of information and communication technologies, violating confidentiality and data security systems by inserting or modifying data to the detriment of a third party, will be punished with imprisonment of four to six years.

Moreover, the Criminal Code sets out crimes for seizing personal data, which are sanctioned with a fine.

9.2 How are personal data breaches regulated in El Salvador? What are the requirements for notification and response?

According to the Law for the Protection of Personal Data, when a data controller becomes aware of a breach or violation of data security (understood as damage, loss, alteration, destruction, illegitimate access or any illicit or unauthorized act), they must notify the State Cybersecurity Agency, the Attorney General's Office and the affected data subjects within a maximum period of 72 hours from when they became aware of the vulnerability, and must begin a review process to determine the magnitude of the impact and the corrective and preventive measures to be taken.

Such measures will depend on the breach committed and the means used to carry out the breach. In cases of breaches committed by computer, this is sanctioned by the special law against cybercrime. In addition, the Criminal Code regulates some breaches and provides sanctions.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

According to the Law for the Protection of Personal Data, infractions are classified as minor, serious, and very serious, with each violation detailed in each category. Their penalties are fines equivalent to 10 to 40 times the minimum monthly wage in the commercial sector. In addition, the penalties for the various violations may include any criminal liability.

According to the Special Law against Computer and Related Crimes, anyone who, without authorization, uses personal data through the use of information and communication technologies, violating confidentiality and data security systems by inserting or modifying data to the detriment of a third party, will be punished with imprisonment of four to six years.

Moreover, the Criminal Code sets out crimes for seizing personal data, which are sanctioned with a fine.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, individuals can exercise their right of action at any time by filing a complaint before the competent authorities; the potential remedies depend on the breach committed and the legislation that regulates it. For example, in the case of financial institutions which have used data for purposes other than those for which authorization was granted, the Banking Law and the Law on the Supervision and Regulation of the Financial System provide that the financial institutions concerned incur joint and several liability for the damages caused to the individuals that provided their data.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Since the law is very recent there are no lawsuits that we know off with regard to privacy non-compliance and there is no regulation, especially in relation to advertising.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in El Salvador?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Companies should be aware of complying with all regulations and also, they should be aware of all their clients' background and have all permissions in place for the use of data with regard to their employees, clients and others.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The major change that has occurred is the approval by the Government in November 2024 of the Law for the Protection of Personal Data—since before this date El Salvador did not have any regulations in regard to data privacy or data protection.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

We believe the challenges lie in being more careful with the information we handle within companies, especially with the information we share with other companies, with banks, and especially with the personal information we provide when contracting services. Data is an extremely important and dangerous tool, so we must strive to safeguard all personal information we disclose and be aware of with whom we share it, as well as the authorizations and/or prohibitions that currently govern us, to avoid any type of violation and/or sanctions.

12.3 What do you envision the privacy landscape will look like in five years?

We believe that in five years, data protection and privacy will be more regulated, and Salvadorans will be more vigilant and more careful with the use, rights, and protection of data. That is to say, currently, companies, especially banks and telephone companies, require people to sign authorizations for the use of data in order to sign contracts, open accounts, and obtain telephone lines. These are mandatory. However, from now on, with the entry into force of the law, we see that it is not mandatory for our data to be disclosed, and we Salvadorans must be more careful with what we sign, the authorizations we grant, and the use of our information we share.



EUROPEAN UNION



1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in the European Union Member States.

Privacy is regulated on two levels: that of the European Union and that of the Member States.

A EU

- (i) On the level of the European Union the most important applicable source of law is the EU General Data Protection Regulation ('GDPR') which became applicable in May 2018. It covers all aspects of privacy law as far as the processing of personal data is concerned.
- (ii) The protection of personal data is also enshrined in the Charter of Fundamental Rights of the European Union, which binds all the institutions, bodies, offices and agencies of the European Union. Moreover, the Member States have to comply with it when implementing EU law. All the European Union's actions must therefore be measured against the Charter, in particular European legislation (Regulations and Directives) and European administration.
- (iii) There is also the ePrivacy Directive, which is not directly applicable, but obliges the Member States to implement its regulations into national law.
Any efforts to modernize the ePrivacy Directive have been shelved for the time being.
- (iv) The regulatory landscape is continuously evolving, with regulations such as the AI and Data Acts.

B Member States

On the level of the Member States there are a variety of different regimes addressing only certain privacy aspects (eg, relating to telecommunication), some of them being the result of EU Directives, others are autonomous acts of each national legislator. In addition, the GDPR contains several opening clauses which allow each Member State to enact national privacy rules to regulate certain limited areas of data processing.

1.2 What are the primary laws regulating privacy in the European Union Member States? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The GDPR is the primary source for the protection of personal data in all EU Member States. This Regulation is directly applicable in all EU Member States without any further enactment or implementation by the national legislator. The GDPR regulates all aspects of the processing of personal data, from its collection, treatment, security, and storage until its deletion. Thus, it also covers the requirements regarding the use of personal data for advertising purposes, information obligations of the advertiser, as well as certain rights of the data subject.

In addition to the GDPR, each Member State has its own national privacy laws (eg, the German Federal Data Protection Act, which provides additional specifications on data protection and enforcement). The ePrivacy Directive also plays a crucial role, as it regulates electronic marketing, cookies, and tracking. Some countries enforce additional advertising laws (eg, the German Unfair Competition Act which places restrictions on unsolicited marketing communications).

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation constitutes an important complementary mechanism within the broader framework of privacy regulation in the European Union, particularly in the context of advertising practices. While the GDPR and the ePrivacy Directive establish the primary legal obligations, various industry-led initiatives seek to ensure compliance and promote responsible data processing practices.

One notable example is the European Advertising Standards Alliance ('EASA'), which oversees adherence to ethical advertising standards across EU Member States. Additionally, the Interactive Advertising Bureau ('IAB Europe') has introduced the Transparency & Consent Framework, a self-regulatory initiative designed to harmonize the process by which advertisers and publishers obtain user consent for data processing, aligning with the requirements of the GDPR.

Self-regulatory measures also play a crucial role in the domain of online behavioral advertising. The European Digital Advertising Alliance administers the AdChoices program, which enhances consumer transparency and control over the use of personal data for targeted advertising. Such initiatives provide market participants with a structured framework for compliance while allowing a degree of flexibility in implementation.

However, self-regulation does not supersede statutory requirements under EU law. Regulatory authorities, including national data protection authorities and the European Data Protection Board, are tasked with overseeing compliance and may impose administrative fines in cases of infringement. As a result, self-regulation functions as a supplementary mechanism that fosters best practices within the industry but operates within the overarching constraints of the European regulatory framework.

1.4 How is privacy law enforced in the European Union Member States? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Pursuant to the GDPR, each EU Member State is required to establish an independent supervisory authority tasked with monitoring and enforcing compliance with data protection law. These authorities, commonly referred to as data protection authorities ('DPA's'), are vested with extensive investigative and corrective powers, including the ability to conduct audits, issue warnings, impose administrative fines, and order the suspension of data processing activities. Their role is central to ensuring the practical enforcement of the GDPR at the national level.

While the GDPR provides a uniform legal framework, its enforcement remains largely decentralized, as implementation and oversight are primarily carried out by the respective national authorities. To ensure a consistent application of the regulation across Member States, the European Data Protection Board ('EDPB') was established. Composed of representatives from each national DPA, the EDPB plays a critical role in issuing guidelines, resolving disputes in cross-border cases, and ensuring coherent interpretation of the GDPR.

Beyond regulatory enforcement, privacy law is also enforced through judicial mechanisms. Courts in each Member State are competent to adjudicate GDPR-related disputes, including actions initiated by data subjects, consumer protection associations, or competitors. Individuals whose rights have been infringed may seek compensation for material and non-material damages resulting from a GDPR violation. This judicial avenue serves as an essential complement to administrative enforcement by allowing affected parties to directly assert their rights.

In addition to regulatory and judicial enforcement, self-regulatory initiatives play a role, particularly in advertising and digital marketing. Industry bodies such as the EASA and IAB Europe have developed codes of conduct and certification mechanisms aimed at fostering GDPR compliance. While these mechanisms do not replace formal enforcement by DPAs or courts, they contribute to a more structured approach to compliance within specific sectors and provide an additional layer of accountability.

Moreover, cross-border enforcement has become increasingly significant, particularly in cases involving multinational corporations. The GDPR introduced the One-Stop-Shop mechanism, which designates the lead supervisory authority based on the location of a company's main establishment within the European Union. However, other concerned DPAs retain the right to intervene where the data subjects in their jurisdiction are affected, ensuring cooperation and consistency in enforcement actions across the European Union.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in the European Union Member States?

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. This will, in fact, subject almost all companies, as well as regulatory bodies, to the GDPR. The only exemptions are specifically listed and comprise, in particular, the processing of personal data in the course of an activity which falls outside the scope of EU law, or the processing of personal data by a natural person in the course of a purely personal or household activity.

2.2 Does privacy law in the European Union Member States apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, it can apply to companies outside the European Union. The GDPR applies to:

- (a) all processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not.
- (b) all controllers and processors not established in the European Union, as far as data subjects in the European Union are concerned, where the processing activities are related to:
 - (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union; or
 - (ii) the monitoring of their behavior, as far as their behavior takes place within the European Union.

Thus, eg, online shops or hotels outside the European Union offering goods or services to data subjects in the European Union will be subject to GDPR.

Non-EU controllers or processors must appoint a representative in the European Union who will act as a point of contact for supervisory authorities and data subjects. The representative must be established in one of the Member States where the data subjects concerned are located.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in the European Union Member States?

Under the GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The GDPR prohibits the processing of:

- (a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- (b) genetic data and biometric data for the purpose of uniquely identifying a natural person;
- (c) data concerning health; or
- (d) data concerning a natural person's sex life or sexual orientation.

The prohibition does not apply if certain strict and conclusive prerequisites, such as explicit consent, are complied with, or if the processing is necessary for the data subject or the controller in the fields of employment, social security and social protection law, or if it is expressly allowed by the national law of a Member State.

When legally handling special categories of personal data under these exceptions, further requirements, such as technical organizational measures or pseudonymization of personal data, need to be fulfilled.

Special conditions apply to the consent of children in relation to information society services. Children must be at least 16 years old to give valid consent to the processing of their personal data. The consent of someone holding parental responsibility is needed in respect of a child below the age of 16. However, the Member States may provide for a lower age for children to give their consent. The controller has to make reasonable efforts to verify in such cases that the special (age) requirements are fulfilled.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The GDPR differentiates between personal data, which falls within its regulatory scope, and data that has been anonymized in such a manner that it no longer allows for the identification of an individual. The treatment of pseudonymized and de-identified data under EU privacy law depends largely on the extent to which re-identification remains possible.

'**Anonymized data**' refers to information that has been processed in such a way that it can no longer be attributed to an identified or identifiable natural person, either by the data controller or any other party. Truly anonymized data is considered to be outside the scope of the GDPR, as it no longer qualifies as personal data. However, anonymization must be irreversible, taking into account current and foreseeable technological advancements that could enable re-identification. If there is a reasonable possibility that anonymized data could be re-identified, it may still be subject to GDPR requirements.

'**Pseudonymization**' refers to the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information. This additional

information must be kept separately and protected through technical and organizational measures to prevent re-identification. Unlike anonymized data, pseudonymized data remains subject to the GDPR, as re-identification remains theoretically possible. Pseudonymization is, however, recognized as a privacy-enhancing measure that can reduce risks to data subjects and facilitate compliance with data protection principles, particularly in the context of data minimization and security.

The term '**de-identified data**' is not explicitly defined in the GDPR but is frequently used to refer to data that has undergone processing to obscure identifying elements. If de-identified data can be reasonably linked back to an individual, either directly or indirectly, it continues to fall within the scope of the GDPR. However, if the de-identification process reaches a standard equivalent to full anonymization, the data may be considered outside the GDPR's regulatory framework.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Obligations vary, depending on the services provided, as well as the type and volume of data and the size of the company. Key obligations are:

- (a) **Transparency:** The obligation to provide information when personal data is collected, what data is collected, as well as giving information regarding the rights of data subjects (eg, in a privacy policy). It is crucial to note that there is no general template for a privacy policy; rather, it should inform about the personal data processed in a way that is adequate in the circumstances.
- (b) **Data security:** Data protection by design and by default; this is especially crucial for websites using cookies or other tracking tools which require the active consent of users.
- (c) **Technical and organizational measures:** Controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In addition, controllers must implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the GDPR and be able to demonstrate this.
- (d) **Assessment:** The obligation to carry out a data protection impact assessment ('DPIA') when new technologies are used, or when the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons. In certain cases, where a DPIA indicates that the processing would result in a high risk, even consultation of the supervisory authority prior to processing may be necessary.
- (e) **Data protection officer:** The obligation to designate and register a data protection officer, unless not required under the applicable national law.
- (f) **Records of processing activities:** The obligation to keep a record of processing activities, containing all relevant data. Records must be in writing (which includes electronic form).
- (g) **Data subject rights:** Controllers must ensure that data subjects can exercise their rights, including the right to access, rectify, erase, and object to data processing, as well as the right to data portability and restriction of processing.
- (h) **Data processing agreements ('DPA's):** Controllers must enter into legally binding agreements with processors to ensure compliance with GDPR requirements. Such contracts must specify processing activities, security measures, and obligations of both parties.

- (i) **Vendor and third-party management:** Companies using third-party service providers to process personal data must ensure that these providers comply with the GDPR and implement appropriate safeguards, such as standard contractual clauses ('SCC's) for international data transfers.
- (j) **Training and awareness:** Organizations must ensure that employees handling personal data receive adequate training on data protection principles, security measures, and the importance of GDPR compliance.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Under the GDPR, companies are assigned roles as either controllers or processors, depending on their data processing activities. These roles determine the extent of their legal obligations.

- (a) A **controller** determines the purposes and means of processing personal data. As the primary entity responsible for compliance, controllers must:
 - (i) establish a legal basis for processing and provide transparent privacy notices;
 - (ii) ensure that data subjects can exercise their rights, including access, rectification, erasure, and objection;
 - (iii) implement appropriate security measures and conduct DPIAs where required; and
 - (iv) conclude DPAs with processors, ensuring compliance with the GDPR.
- (b) A **processor** acts solely on behalf of the controller and must:
 - (i) process personal data only under the controller's instructions;
 - (ii) implement security measures and ensure compliance by sub-processors; and
 - (iii) assist controllers in fulfilling data protection obligations, such as responding to data subject requests.

In cases where two or more entities jointly determine processing purposes and means, they qualify as joint controllers and must define their respective responsibilities.

The distinction between controllers and processors is crucial, as controllers bear the primary legal responsibility for compliance, while processors must ensure secure and lawful processing within the framework set by the controller. Misclassification can lead to regulatory scrutiny and penalties.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Under the GDPR, the processing of personal data requires a lawful basis. Controllers must establish and document a valid legal justification before collecting or using personal data, ensuring transparency (see questions 4.1 and 5).

The lawful bases for processing personal data are:

- (a) **Consent:** The data subject has freely given, specific, informed, and unambiguous consent. It must be obtained through a clear affirmative action and can be withdrawn at any time. Explicit consent is required for special categories of personal data under Article 9(2)(a) GDPR.
- (b) **Performance of a contract:** Processing is necessary to fulfill a contract with the data subject or to take steps at their request before entering into a contract.
- (c) **Compliance with a legal obligation:** Processing is required to meet a legal duty imposed by EU or national law.

- (d) **Protection of vital interests:** Processing is necessary to protect a person's life or physical safety, typically in medical emergencies where the individual cannot provide consent.
- (e) **Public interest or official authority:** Processing is required for tasks carried out in the public interest or under official authority.
- (f) **Legitimate interests:** Processing is justified when necessary to pursue the legitimate interests of the controller or a third party, provided this does not override the rights of data subjects.

For special categories of personal data, additional conditions must be met, such as explicit consent, legal claims, or substantial public interest (see question 3.2).

Failure to establish a lawful basis renders processing unlawful and may result in regulatory action, fines, or invalidation of data processing activities. Controllers must ensure transparency and document their legal basis in accordance with GDPR requirements.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the GDPR, companies processing personal data for advertising purposes must provide clear and transparent privacy notices. These notices must inform data subjects about the purpose, scope, and legal basis of the processing.

The privacy notice must include:

- (a) **Identity and contact details of the controller:** The name and contact details of the data controller and, where applicable, the data protection officer.
- (b) **Purpose and legal basis:** A clear explanation of why personal data is processed for advertising, specifying whether it is based on consent or legitimate interest. If legitimate interest applies, the specific interest must be disclosed.
- (c) **Categories of personal data:** If the data was not collected directly from the individual, the type of data processed (eg, browsing behavior, demographic data) must be specified.
- (d) **Recipients of data:** Disclosure of third parties receiving the data, such as advertising networks or social media platforms.
- (e) **International data transfers:** If personal data is transferred outside the European Economic Area ('EEA'), companies must indicate the transfer mechanisms in place (eg, standard contractual clauses).
- (f) **Retention period:** The duration of data storage or the criteria used to determine it.
- (g) **Rights of the data subject:** Information on data subject rights, including access, rectification, erasure, objection, and withdrawal of consent where applicable.
- (h) **Right to object to direct marketing:** A specific notice that individuals have the right to object to data processing for advertising purposes.
- (i) **Automated decision-making and profiling:** If data is used for automated decision-making, including profiling, companies must describe the logic involved and its potential impact.
- (j) **Source of data:** If personal data is obtained from third parties, the source must be disclosed.

Privacy notices must be concise, written in clear language, and easily accessible. This is particularly relevant for online advertising, where companies must ensure transparency regarding the use of tracking technologies and provide mechanisms for users to manage their preferences.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Under the GDPR, consumers have several rights regarding the processing of their personal data in advertising contexts. These rights ensure transparency, control, and protection against misuse of personal data:

- (a) **Right to be informed:** Consumers must be provided with clear and transparent information on how their data is collected, used, and shared for advertising purposes.
- (b) **Right of access:** Individuals can request confirmation as to whether their data is being processed and obtain a copy of the personal data held about them.
- (c) **Right to rectification:** Consumers can request the correction of inaccurate or incomplete personal data.
- (d) **Right to erasure ('right to be forgotten'):** Individuals may request the deletion of their personal data, particularly when processing is based on consent or is no longer necessary for its original purpose.
- (e) **Right to restrict processing:** Consumers can request the restriction of processing under certain conditions, such as when the accuracy of data is contested.
- (f) **Right to object:** Consumers have the absolute right to object to processing for direct marketing purposes, including profiling related to such marketing.
- (g) **Right to data portability:** If processing is based on consent or contract, individuals can request their personal data in a structured, commonly used, and machine-readable format and have it transferred to another controller.
- (h) **Rights related to automated decision-making and profiling:** Consumers have the right not to be subject to solely automated decisions, including profiling, that produce legal or similarly significant effects on them, unless specific exemptions apply.

Organizations engaged in advertising activities must ensure mechanisms for exercising these rights and respond to requests within one month.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the GDPR and the ePrivacy Directive, companies must obtain consent or provide opt-out mechanisms for advertising activities depending on the nature of the data processing involved:

- (a) **Consent requirement:** Explicit, informed, and freely given consent is required before processing personal data for targeted advertising, tracking, or using cookies and similar technologies. Consent must be obtained through a clear affirmative action and can be withdrawn at any time.
- (b) **Legitimate interest and opt-out:** Companies may rely on legitimate interest for certain advertising activities, such as direct marketing via postal mail or contextual advertising, provided a balancing test is conducted. In such cases, consumers must be informed of their right to object and offered an opt-out mechanism.
- (c) **Electronic marketing communications:** Prior consent is required for email, SMS, and automated marketing calls unless an existing customer relationship applies, in which case an opt-out must be provided.
- (d) **Behavioral advertising and tracking technologies:** The use of cookies, pixels, and similar tracking tools requires prior consent unless they are strictly necessary for website functionality.

Companies must implement transparent consent mechanisms, such as cookie banners or preference management tools, and maintain records of consent. Opt-out options must be easily accessible and effective, ensuring compliance with consumers' rights to object (see question 5.2).

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Under the GDPR, companies engaging vendors and third parties in advertising, such as advertising agencies, demand-side platforms ('DSP's), supply-side platforms ('SSP's), and data providers, must ensure compliance with data protection requirements. as follows:

- (a) **Controller-processor relationship:** If a third party processes personal data on behalf of a controller, a DPA is required, specifying the scope, security measures, and obligations regarding data protection.
- (b) **Joint controllers:** If multiple parties jointly determine the purposes and means of processing, they must define their respective responsibilities in a transparent agreement.
- (c) **Third-party data sharing:** If personal data is shared with vendors, data subjects must be informed of the recipients and the legal basis for such processing. If data is obtained from third parties, its source must be disclosed.
- (d) **International data transfers:** If vendors or third parties are located outside the EEA, appropriate safeguards, such as SCCs or adequacy decisions, must be in place.
- (e) **Consent and opt-out obligations:** If vendors engage in tracking, retargeting, or behavioral advertising, valid consent must be obtained where required and opt-out mechanisms must be available.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Under the GDPR, companies disclosing or receiving personal data from vendors or third parties must ensure compliance through appropriate contractual arrangements as follows:

- (a) **DPA's:** When engaging a processor, controllers must establish a written agreement specifying processing purposes, security measures, confidentiality obligations, and the processor's duty to assist with compliance. Sub-processors require prior authorization.
- (b) **Joint controller agreements:** Where two or more controllers jointly determine the purposes and means of processing, they must define their respective responsibilities, including obligations regarding transparency and handling data subject rights.
- (c) **Third-party data sharing:** If personal data is shared with third parties, the privacy notice must specify the recipients and the legal basis for disclosure. If data is received from third parties, its source must be disclosed.
- (d) **International data transfers:** If personal data is transferred outside the EEA, companies must implement safeguards such as SCCs, binding corporate rules ('BCR's), or rely on adequacy decisions.
- (e) **Confidentiality and security:** Contracts must require vendors to implement appropriate technical and organizational measures to ensure data security and compliance with GDPR principles.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Under the GDPR, companies must implement due diligence measures to ensure compliance with data protection principles, particularly when engaging third parties or processing personal data for advertising purposes. In particular:

- (a) **Vendor assessment:** Before engaging processors, companies must evaluate their data protection practices, security measures, and compliance history, ensuring a valid DPA is in place;
- (b) **Lawful basis review:** Companies must document the legal basis for processing, particularly when relying on legitimate interest for advertising activities, which requires a balancing test;
- (c) **Transparency and consent management:** Organizations must provide clear privacy notices and obtain valid consent where required, ensuring opt-out mechanisms for direct marketing;
- (d) **Security and risk management:** Adequate technical and organizational measures must be in place to protect personal data against breaches and unauthorized access; and
- (e) **DPIAs:** These are required when processing is likely to result in a high risk to data subjects, such as large-scale profiling, tracking, or behavioral advertising using sensitive data. If high residual risk remains, consultation with the supervisory authority may be necessary.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing, including emails, text messages, and push notifications, is regulated under the GDPR and the ePrivacy Directive. In particular:

- (a) **Consent requirement:** Direct marketing communications generally require prior, freely given, and informed consent. Consent must be explicit, obtained before sending marketing messages, and easily revocable.
- (b) **Soft opt-in exception:** Organizations may send marketing communications to existing customers without prior consent if the marketing relates to similar products or services, the customer provided their contact details during a sale, and an opt-out option is offered in every communication.
- (c) **Right to object:** Data subjects have the right to object to direct marketing at any time. Upon objection, processing must cease immediately.
- (d) **Identification and transparency:** Marketing messages must clearly identify the sender, provide contact details, and include an easy opt-out mechanism.

Member States may impose additional restrictions on direct marketing, such as requirements for do-not-call lists or additional consumer protection.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies such as cookies, pixels, and software development kits ('SDK's) are regulated under the ePrivacy Directive and the GDPR. Note, in particular:

- (a) **Consent requirement:** The storage or access of information on a user's device, including cookies and similar tracking technologies, requires prior consent unless strictly necessary for providing a requested service. Consent must be freely given, informed, and unambiguous, typically obtained through a compliant cookie banner.

- (b) **Transparency obligations:** Organizations must clearly inform users about the purpose, duration, and recipients of tracking data, including any third-party involvement, through a privacy or cookie policy.
- (c) **Right to withdraw consent:** Users must be able to withdraw consent easily at any time, and rejecting tracking should not affect access to essential services.
- (d) **Legitimate interest exemption:** Certain first-party analytics may rely on legitimate interest, provided a balancing test is conducted and users are given an opt-out mechanism.

Many EU DPAs have issued guidance and fines for non-compliant cookie practices, emphasizing the requirement for clear, affirmative user consent.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions involving personal data processing are subject to the GDPR and, where applicable, the ePrivacy Directive. In particular:

- (a) **Lawful basis:** Processing must be based on a valid legal basis, typically consent (eg, personalized marketing) or contractual necessity (eg, administering loyalty benefits). If relying on legitimate interest, a balancing test must be conducted.
- (b) **Transparency:** Participants must be clearly informed about data collection, purposes, retention periods, and third-party sharing through a privacy notice.
- (c) **Profiling and automated decision-making:** If loyalty programs involve profiling or automated decisions with legal or significant effects, additional safeguards, such as explicit consent or human intervention, may be required.
- (d) **Data minimization and retention:** Companies must collect only necessary data and define appropriate retention periods, ensuring deletion when no longer needed.
- (e) **Opt-out and consent withdrawal:** Participants must have the right to withdraw consent or opt out of marketing communications at any time.
- (f) **Fair processing principles:** Any incentives tied to data collection should comply with fairness principles, ensuring that participation is genuinely voluntary and that consent is not a condition for receiving core program benefits.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing involving personal data processing are regulated under the GDPR and the ePrivacy Directive as follows:

- (a) **Legal basis:** Processing personal data for targeted advertising or influencer marketing requires a valid legal basis, such as consent for personalized ads or legitimate interest for non-intrusive marketing, subject to a balancing test.
- (b) **Transparency and privacy notices:** Users must be informed about data collection, targeting methods, and third-party data sharing through clear privacy policies.
- (c) **Consent for tracking:** The use of cookies, pixels, and similar tracking technologies for behavioral advertising requires prior consent, except where strictly necessary.
- (d) **Influencer disclosures and fairness principles:** Endorsements must be clearly identifiable as advertising to ensure transparency, in line with consumer protection laws and platform policies.
- (e) **User rights and opt-out:** Users must be able to withdraw consent and object to the use of their data for targeted advertising at any time.

- (f) **DPA:** Brands and influencers collaborating with third-party marketing platforms must ensure compliance through contractual agreements governing data processing.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Privacy law, particularly the GDPR and the ePrivacy Directive, imposes strict requirements on targeted advertising, including behavioral and personalized advertising, while applying a more lenient approach to contextual advertising:

- (a) **Legal basis for targeted advertising:** Processing personal data for behavioral or personalized advertising requires a valid legal basis, typically explicit consent. If legitimate interest is relied upon, a balancing test must be conducted, and users must be given the right to object.
- (b) **Tracking and profiling requirements:** Organizations must inform users about data collection, profiling methods, and third-party data sharing. If automated decision-making significantly affects individuals, additional safeguards may be required.
- (c) **Consent for tracking technologies:** The use of cookies, tracking pixels, and similar technologies for behavioral advertising requires prior consent, except when strictly necessary for basic website functionality.
- (d) **Contextual advertising distinction:** Contextual advertising, which is based on the content of a webpage rather than user behavior, does not involve the processing of personal data and is therefore not subject to GDPR consent requirements. However, general transparency obligations may still apply.

Many EU data protection authorities have issued guidance reinforcing the necessity of valid consent for behavioral advertising, and non-compliance has led to significant fines.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are subject to the GDPR and, where applicable, the ePrivacy Directive. These technologies involve data matching, anonymization, and controlled data sharing, raising significant privacy considerations, including:

- (a) **Legal basis for processing:** Identity resolution and data matching require a valid legal basis, typically consent or legitimate interest, subject to a balancing test and opt-out rights.
- (b) **Transparency and purpose limitation:** Organizations must inform individuals about data collection, matching methods, and intended uses. If data is obtained from third parties, its source must be disclosed.
- (c) **Anonymization and pseudonymization:** Data used in clean rooms should be pseudonymized or anonymized to minimize privacy risks. However, pseudonymized data remains within the scope of GDPR if re-identification is possible.
- (d) **Third-party data sharing:** If identity resolution involves external providers, DPAs must be in place, defining processing obligations and security measures.
- (e) **Restrictions on automated decision-making:** If identity resolution leads to profiling or automated decisions with legal or similarly significant effects, additional safeguards such as human review or explicit consent may be required.
- (f) **ePrivacy Directive considerations:** Where cookies or tracking technologies enable identity resolution, prior user consent is required.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is subject to the GDPR and the ePrivacy Directive, as it involves the processing of personal data, often through tracking technologies. In particular:

- (a) **Legal basis for processing:** Collecting and using location data for advertising requires a valid legal basis, typically explicit consent, especially for precise geolocation tracking. Legitimate interest may apply in limited cases, subject to a balancing test and opt-out rights.
- (b) **Consent for tracking:** The use of cookies, GPS, Wi-Fi, or Bluetooth for location tracking requires prior user consent, unless strictly necessary for a requested service.
- (c) **Transparency obligations:** Companies must clearly inform users about the collection, purpose, retention period, and sharing of location data, including third-party recipients.
- (d) **Minimization and security:** Location data must be limited to what is necessary for the stated purpose and protected through appropriate security measures to prevent unauthorized access.
- (e) **Special protections for children:** The use of location data for advertising targeting minors requires heightened safeguards, including verifiable parental consent.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are entities that collect, aggregate, and sell or share personal data from various sources, often without direct interaction with data subjects. Their activities are regulated under the GDPR when processing personal data of individuals in the European Union as follows:

- (a) **Legal basis for processing:** Data brokers must establish a lawful basis for processing, typically legitimate interest, subject to a balancing test, or consent when required.
- (b) **Transparency obligations:** When obtaining data from third-party sources, brokers must inform data subjects about the data collection, processing purposes, categories of data, and recipients.
- (c) **Right to object and opt-out:** Data subjects have the right to object to processing, particularly for direct marketing, requiring brokers to cease processing upon request.
- (d) **Accuracy and data minimization:** Data brokers must ensure data accuracy, limit processing to what is necessary, and delete outdated or incorrect information.
- (e) **Data subject rights:** Individuals have the right to access, rectify, erase, and restrict the processing of their personal data, and brokers must implement mechanisms to facilitate these rights.

Non-compliance can result in fines of up to €20 million or 4% of global annual turnover. Regulatory scrutiny of data brokers has increased, with several enforcement actions highlighting failures in transparency and lawful processing.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors is subject to strict privacy protections under the GDPR and, where applicable, the ePrivacy Directive, due to the heightened vulnerability of minors. In particular:

- (a) **Consent requirements:** Processing personal data of children under 16 (or a lower national threshold, minimum 13) for information society services, including targeted advertising, requires verifiable parental consent.
- (b) **Transparency obligations:** Privacy notices must be child-friendly, ensuring clear and accessible explanations of how personal data is used for advertising.

- (c) **Profiling and automated decision-making:** Automated profiling of minors for targeted advertising is generally discouraged, and if conducted, specific safeguards must be in place.
- (d) **Use of tracking technologies:** Cookies and similar technologies for behavioral advertising targeting minors require prior consent, as children cannot be expected to provide informed decisions regarding tracking.
- (e) **Fairness and best interests principle:** Processing children's data for advertising must not exploit their lack of awareness of privacy risks.

Regulators emphasize heightened protection, transparency, and parental control over minors' data. Organizations must implement robust safeguards, obtain valid consent, and ensure compliance with stricter standards when engaging in child-directed advertising.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Profiling and the use of artificial intelligence ('AI') or automated decision-making in advertising are regulated under the GDPR to ensure fairness, transparency, and the protection of individual rights. The following apply:

- (a) **Legal basis for processing:** Profiling and AI-driven advertising require a lawful basis, typically consent or legitimate interest, subject to a balancing test and opt-out rights.
- (b) **Transparency and data subject rights:** Organizations must inform individuals about profiling, its purposes, and any meaningful logic behind AI-driven decision-making. Data subjects have the right to access their data and request an explanation of automated processing.
- (c) **Restrictions on solely automated decision-making:** Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if the decision produces legal effects or similarly significant consequences, unless explicit consent is obtained or a contractual necessity applies.
- (d) **Accuracy and fairness:** AI-based advertising must ensure data accuracy, avoid bias, and apply appropriate safeguards to prevent unfair discrimination.
- (e) **Right to object and opt-out:** Individuals must be given the right to object to profiling for advertising purposes and withdraw consent at any time.

7.11 Are there other specific advertising practices that you wish to discuss?

See the chapters for individual Member States.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Any transfer of personal data within the EEA is subject to the general provisions of the GDPR, including the requirement for a valid legal basis and compliance with data security obligations. This applies equally to transfers within corporate groups.

For transfers of personal data outside the EEA, the following mechanisms must be observed in addition to having a legal basis:

- (a) **Transfers based on an adequacy decision:** The European Commission may determine that a third country ensures an adequate level of data protection. As of now, adequacy decisions exist for Andorra, Argentina, Canada (commercial organizations), Guernsey, Faroe Islands, Isle of Man, Israel, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.
- (b) **Transfers subject to appropriate safeguards:** In the absence of an adequacy decision, personal data may be transferred only if the controller or processor implements appropriate safeguards, ensuring enforceable data subject rights and legal remedies. The most relevant safeguards include:
 - (i) **SCCs:** Adopted by the European Commission, SCCs remain a widely used transfer mechanism but require additional risk assessments and supplementary security measures following the Schrems II ruling (C-311/18); and
 - (ii) **BCRs:** Approved by data protection authorities, BCRs enable multinational organizations to transfer data within their group under uniform privacy standards.
- (c) **Derogations for specific situations:** If neither an adequacy decision nor appropriate safeguards apply, transfers may occur only under limited exceptions, such as:
 - (i) explicit consent of the data subject, provided they are informed of the risks;
 - (ii) necessity for contractual performance between the data subject and the controller;
 - (iii) important public interest recognized by EU or national law;
 - (iv) legal claims requiring cross-border data transfers; or
 - (v) vital interests of individuals in emergencies.

Certain jurisdictions impose additional restrictions on data transfers. For example, transfers to data importers in the United States that have not been certified according to the EU-US Data Privacy Framework require supplementary measures due to concerns raised in Schrems II, while transfers to countries with state surveillance risks must be assessed carefully.

Organizations must conduct transfer impact assessments, implement supplementary technical and organizational safeguards, and ensure ongoing compliance with evolving regulatory requirements.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The above described requirements for data transfers also apply to discovery or similar proceedings making complying with such requirements challenging at times.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in the European Union Member States? Are there minimum standards? Does this differ by sector or size of the entity?

Different measures need to be taken in accordance with the data security rules contained in GDPR and the national laws; in comparison to data protection, data security is not limited to personal data. Measures include, inter alia, pseudonymization and encryption, as well as system resilience or availability and access. These measures need to be evaluated regularly and, if necessary, adapted. All technical tools used need to be state of the art.

Data security is complemented by technical and organizational measures, which require a hands-on approach to securing data in companies through appropriate means, as well as technical and organizational measures, such as a clean desk policy, limited access rights, or locked bins for sensitive material. This is further specified in the GDPR and in national laws.

Typically, national data protection authorities have issued guidelines on data security.

9.2 How are personal data breaches regulated in the European Union Member States? What are the requirements for notification and response?

In the GDPR, data breaches are primarily regulated by notification requirements. In case of a breach, companies are required to inform:

- (a) the data subject without delay, if the breach is likely to result in a high risk to the rights and freedoms of natural persons; and
- (b) the supervisory authority within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Non-compliance with the GDPR can result in significant administrative fines and other enforcement measures imposed by DPAs as follows:

- (a) **Administrative fines:** The GDPR distinguishes between two levels of fines:
 - (i) up to €10 million or 2% of global annual turnover for less severe violations, such as failure to maintain proper records, implement security measures, or conduct impact assessments;
 - (ii) up to €20 million or 4% of global annual turnover for serious violations, including unlawful processing, lack of valid consent, infringement of data subject rights, or unauthorized international data transfers.
- (b) **Corrective measures:** Supervisory authorities may issue warnings, reprimands, processing bans, or orders to rectify non-compliance, including the suspension of data flows.
- (c) **Civil liability:** Data subjects can claim compensation for material and non-material damages resulting from GDPR violations. Organizations may be held liable for damages caused by their processors.
- (d) **Criminal penalties:** Certain EU Member States impose criminal sanctions for severe breaches, such as unlawful data processing or intentional misuse of personal data.

Regulatory scrutiny has intensified, with high-profile enforcement actions against major companies, emphasizing the need for compliance with GDPR obligations. Organizations must implement robust compliance frameworks, risk assessments, and accountability measures to mitigate legal and financial risks.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under the GDPR, consumers (data subjects) have a private right of action and can seek the following remedies for violations of their data protection rights:

- (a) **Right to lodge a complaint:** Data subjects can file complaints with their national supervisory authority, which may investigate and impose corrective measures.

- (b) **Judicial remedies:** Individuals have the right to challenge supervisory authority decisions or directly initiate legal proceedings against controllers or processors for GDPR violations.
- (c) **Right to compensation:** Data subjects can claim compensation for material and non-material damages resulting from unlawful data processing. Liability may extend to both controllers and processors.
- (d) **Collective actions:** Some EU Member States allow representative actions by consumer protection organizations or data protection advocacy groups, particularly in large-scale data breaches.

Enforcement trends indicate growing litigation related to data breaches, unlawful tracking, and misuse of personal data. Organizations must ensure compliance with GDPR principles to mitigate litigation risks.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement of privacy laws in the advertising sector has been notably active, with regulators and courts addressing various non-compliance issues. Significant enforcement actions and lawsuits include:

- **LinkedIn fined for targeted advertising practices:** In October 2024, the Irish Data Protection Commission imposed a €310 million fine on LinkedIn for processing personal data without a lawful basis for targeted advertising, violating the GDPR.
- **Meta prohibited from using sensitive data for ads:** The European Court of Justice ruled that Meta (Facebook's parent company) cannot utilize users' publicly available data regarding sexual orientation for personalized advertising without explicit consent, reinforcing the GDPR's data minimization principles.
- **Amazon sued over data collection practices:** In January 2025, Amazon faced a lawsuit alleging unauthorized collection of personal and location data through third-party mobile apps for advertising purposes, raising significant privacy concerns.
- **Apple settles over Siri privacy violations:** Apple agreed to a \$95 million settlement in response to allegations that its voice assistant, Siri, improperly recorded user conversations without consent and shared the data with advertisers, highlighting issues of inadvertent data collection.
- **Google's ad platform enables sensitive targeting:** Investigations revealed that Google's Display & Video 360 platform allowed advertisers to target users based on sensitive information, such as health conditions and national security roles, leading to scrutiny over inadequate enforcement of data protection policies.

These cases underscore the heightened regulatory focus on ensuring that advertising practices comply with privacy laws, particularly concerning lawful data processing, explicit consent, and the protection of sensitive personal information.

In addition, there are more and more private enforcement actions for damages under the GDPR. Most of those are brought by experienced consumer protection law firms. Further, increasing numbers of alternative legal services providers are emerging.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in the European Union Member States?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

See the chapters for individual Member States.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

See the chapters for individual Member States.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The AI Act, Data Act and other digital regulations were launched as part of the European Digital Single Market.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Keeping track of the emerging regulations in more and more countries outside of the EEA.

12.3 What do you envision the privacy landscape will look like in five years?

See the chapters for individual Member States.

 AUSTRIA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Austria.

In Austria, the strict privacy rules of the GDPR are applicable. Thus, natural persons are granted rights under the GDPR and controllers and processors have to adhere to its strict standards.

Apart from that, the right to privacy is a fundamental right under the Austrian Privacy Act and under the Charter of Fundamental Rights of the European Union that is granted under the Constitution.

The right to data protection under the Austrian Privacy Act is a fundamental right of every individual. It is not linked to Austrian citizenship, nor is it limited to natural persons; thus, legal entities are also protected. However, the protection of legal entities under the Austrian Privacy Act is less extensive than the GDPR, especially since the Privacy Act contains fewer rights for data subjects.

1.2 What are the primary laws regulating privacy in Austria? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

In the first place, the GDPR is directly applicable in Austria.

Austria's Privacy Act 2000 was amended in 2018 to implement changes due to the GDPR entering into force. Austria made very little use of the opening clauses set out in the GDPR.

Apart from that, privacy regulations can be found in various other statutes, eg in laws applying to scientific research etc.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

See the European Union chapter.

1.4 How is privacy law enforced in Austria? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

First of all, the Austrian Data Protection Authority ('DSB'), as established by the Austrian Privacy Act, is responsible for enforcing privacy laws, and has extensive rights and may impose fines. It is the supervisory body pursuant to the GDPR.

Secondly, the Austrian courts may rule on privacy matters. They are also competent to award damages for data breaches.

A data subject may pursue both paths in any privacy matter, ie, seek help from the courts and from the DSB.

Since January 1, 2025, the Parliamentary Data Protection Committee ('PDK') has been responsible for data protection in the legislative sphere in Austria as an independent national supervisory authority. It was established to monitor the processing of personal data by legislative bodies and to ensure legal protection. Any data subject may lodge a complaint with the PDK if they believe that the processing of their personal data by a legislative body violates the GDPR or the Austrian Privacy Act.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Austria?

A company must adhere to the strict privacy rules when processing data of individuals, if:

- (a) the company is located in Austria;
- (b) offers goods or services in Austria; or
- (c) monitors the behavior of data subjects within Austria.

2.2 Does privacy law in Austria apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Privacy laws apply to companies outside Austria pursuant to the rules set forth in the GDPR. Thus, if companies outside Austria offer goods or services in Austria, or monitor the behavior of data subjects within Austria, Austrian privacy laws apply. If such companies are located outside the European Union, or do not have an establishment in the EU processing the data, then such companies are under a duty to appoint a representative in an EU member state.

See also the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Austria?

'Personal data' has the wide meaning set forth in the GDPR. See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The obligations of a controller or processor are those set out in the GDPR. Generally, each controller and processor must:

- (a) ensure transparency and the lawful processing of data;
- (b) maintain a record of processing activities;
- (c) appoint a privacy officer when required under the GDPR (Austria does not have any stricter rules than under the GDPR) and register the privacy officer with the DSB;
- (d) conduct a risk impact assessment where required under the GDPR;
- (e) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk; and

- (f) maintain sufficient documentation to be able to demonstrate compliance of the processing activities with the GDPR and execute the necessary contracts (eg, with processors, joint controllers or, where required, with recipients of personal data in countries outside the EU).

In more detail, and with regard to advertising, each controller has to:

- (g) set up a privacy statement informing data subjects about the processing of their personal data as well as their rights under the GDPR;
- (h) execute joint controller agreements with social media platforms (when used by the controller);
- (i) execute controller–processor agreements (when processors are employed);
- (j) use cookies in line with the legal requirements (see question 8.2);
- (k) ask for data subjects' consent for certain marketing activities (such as promotional emails) etc; and
- (l) obey the GDPR requirements and rules for data transfers to third countries (eg, when employing enterprises like Mail Chimp for marketing purposes or storing data in clouds).

Furthermore, each controller and processor should have a privacy policy laying down the applicable principles concerning privacy issues, and instruct employees regularly involved in data processing about privacy, as well as have them sign a privacy statement.

There is case law stating that the privacy statement serves only as information and therefore does not have to be accepted by customers. If companies, for example, include a checkbox in online forms to indicate that the privacy policy has been 'accepted' or 'acknowledged,' this can have negative consequences. The privacy policy is then considered a contract, which is subject to strict content control (especially in the case of consumers). In such case, consumer protection association are entitled to challenge privacy policies before the courts. It is therefore advisable to provide the privacy policy for information purposes only and not to require confirmation or acceptance.

See also the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Individuals (data subjects) have the rights specified in the GDPR. See the European Union chapter.

If individuals are denied these rights, they can enforce them either through the ordinary courts or by lodging a claim with the DSB or both.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

For marketing communications, again, the GDPR applies. See the European Union chapter.

Under the GDPR, marketing communication is only permitted if the processing of the individual's personal data (eg, email address) is lawful. Usually this either requires the individual's consent or, in some cases, that the legitimate interests pursued by the controller or by a third party are not outweighed by those of the individual. If the data subject is a child, this balancing of interests is usually in favor of the child.

In addition, for electronic communication, the Telecommunication Act applies. The Telecommunication Act implemented the regulations of the EU ePrivacy Directive. Under the Act, the prior consent of the individual is required in almost all cases.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies are subject to the rules of the GDPR. See the European Union chapter.

Cookies are also regulated by the Telecommunications Act (see also the question 7.1).

Tracking generally requires the consent of the data subject. In this context, it is important to note that consent must be given actively. It is not sufficient to use, eg, a cookie banner informing data subjects about the tracking and to require data subjects to disable the same if they do not actually consent to the use of cookies.

Only ‘necessary cookies’—ie, those needed to be able to provide the services offered online—may be used without the data subject’s consent.

The data subject must also be informed in detail about the tracking methods, in particular about the various cookies that are being used.

In a decision that has attracted attention throughout Europe, the Austrian DSB has deemed the use of Google Analytics to be unlawful. The reason was that Google was unlawfully transferring the collected data to a third country, namely the USA.

In 2022, the DSB initiated an official investigation into Google Fonts and the related processing of personal data after an Austrian lawyer had claimed damages and omission from a large number of companies for using Google Fonts on their websites. The DSB found that the transparency requirements of the GDPR were violated when integrating Google Fonts. The decision emphasized the importance of transparency and the need to provide users with comprehensive information about data processing. Companies should adapt their data processing practices accordingly, especially when integrating services such as Google Fonts. If Google Fonts are dynamically integrated, the explicit and informed consent of users must be obtained prior to data transfer.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no special rules from a privacy perspective, other than those under the GDPR. Transparency and the lawful processing of personal data under Article 6 of the GDPR are required. Under certain circumstances, the data subject’s consent may be linked to the right to participate in sweepstakes or the like.

7.4 How is social media and influencer marketing regulated under privacy law?

Again, the GDPR applies. See the European Union chapter.

Otherwise there are no specific rules. Social media platforms are considered to be joint controllers, with the consequence that companies using social media platforms need to enter into a joint controller agreement with the social media operator (eg, Facebook).

Otherwise, transparency rules are particularly relevant. The data subject’s consent may be required for social media activities.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Again, the rules of the GDPR apply. See the European Union chapter.

Targeting and behavioral advertising usually require the data subject’s consent. Contextual advertising does not.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are subject to the GDPR and, where applicable, the ePrivacy Directive, implemented by the Telecommunication Act. See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

Again, this is subject to the GDPR and, where applicable, the ePrivacy Directive, implemented by the Telecommunication Act. See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

The Austrian Trade Law contains special rules for data brokers. Generally, the GDPR is applicable for them, too. Address publishers and direct marketers are allowed to obtain personal data for their activities from publicly available information, by interviewing data subjects, from customer and interest file systems of third parties, or from marketing file systems of other address publishers and direct marketing companies, provided that this is done in compliance with the principle of proportionality for the preparation and implementation of marketing campaigns of third parties, including the design and dispatch of advertising material or list broking. This right is, however, limited to narrowly defined categories of data. For the processing of sensitive data, the data subject's consent is required.

7.9 How is advertising to children and minors regulated under privacy law?

In Austria, minors aged 14 and over can consent to the processing of their personal data if it relates to information society services (eg, social media, online shops, streaming, etc). Before their 14th birthday, the consent of their legal representatives (usually their parents) is required.

This age limit is set out in the Austrian Privacy Act and makes use of the option provided by the GDPR to lower the age limit at national level.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

No, except for newsletters—see question 10.3.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Again, the GDPR applies.

To begin with, data transfers are only permitted if the processing of personal data and the transfer are lawful. For instance, between group companies, a transfer could be lawful because the legitimate interests of the group outweigh the interests of the data subjects whose personal data is being transferred.

Transfers to countries outside the EU are subject to the strict rules under the GDPR. See the European Union chapter. In general, privacy and the data subject's rights must be adequately secured.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Austria? Are there minimum standards? Does this differ by sector or size of the entity?

Generally speaking, security is mainly covered by the rules laid down in the GDPR. Each controller and processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

See the European Union chapter.

9.2 How are personal data breaches regulated in Austria? What are the requirements for notification and response?

Again, there are no special rules other than those set out in the GDPR. See the European Union chapter.

Furthermore, the controller must document any personal data breaches, noting the facts relating to the personal data breach, its effects and the remedial action taken.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

There is a wide range of penalties and sanctions, from a warning by the DSB to the highest fines under the GDPR (administrative fines up to €20 million, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher).

The Austrian Data Protection Act sets out additional fines for certain administrative offences under the Act.

As foreseen under the GDPR, individuals may claim damages for data breaches, which—especially in cases where numerous data subjects are affected—can be higher than the fines under the GDPR.

10.2 Do consumers have a private right of action? What remedies are available to them?

Individuals may lodge claims with the courts and with the DSB:

- (a) the courts may award damages and/or prohibit the further processing of data;
- (b) the DSB may impose fines and also prohibit the further processing of data.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The DSB is very active. In 2024, it handled 6,226 cases (complaints, ex officio investigations, administrative penalty proceedings, reports of data breaches, etc). Approximately 20% of the cases were closed, with the majority resulting in a decision. A total of 73 fines were imposed, amounting to €1,684,230. The highest (legally binding) individual fine was €1,500,000 for the unlawful operation of a video surveillance system.

The highest fine ever imposed by the DSB was a penalty of €18 million against Austrian Postal Service. This penalty was imposed for unlawful data processing (in particular the storage and evaluation of political affiliations). However, this penalty decision is not final; Austrian Post has lodged an appeal.

The highest final fine that has actually been enforced is €50,000. This was imposed on a company in the medical sector for, among other things, violations of reporting obligations and failure to appoint a data protection officer. In another case, a penalty of €4 million originally imposed on a credit institution was reduced to €50,000 by the Federal Administrative Court.

Generally, in 2024, in many cases the fines imposed by the DSB were significantly reduced by the Court of Appeal.

In a decision dated September 11, 2024, the DSB issued a decision on the sending of newsletters, for example. In the specific case, a voter group had collected email addresses from supporters while gathering statements of support for an initiative to reduce fees. These email addresses were then used to send a newsletter about the group's political activities without obtaining separate consent. The DSB clarified that mere support for a political cause cannot automatically be regarded as consent to receive newsletters. Rather, legally valid consent under the GDPR requires a clear, affirmative action and prior information to the data subjects. 'Implicit' or 'implied' consent is not sufficient under the GDPR.

It is also particularly important that even if an explicit declaration of consent had been given, it would have been invalid if it had not been clearly separated from the support for the political cause. Consent to receive the newsletter must therefore be obtained separately and independently of other declarations.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Austria?

The right to privacy is a fundamental right under Austria's constitution, which extends protection to corporations and other legal persons.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

None.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, the ECJ has clarified some open questions regarding the GDPR, although not all of them. This includes the issue of damages. Damages for violations of the GDPR have not yet played a major role in Austria, but such cases are to be expected in the future.

A new development is the establishment of the PDK (see question 1.4), which is responsible for compliance with and enforcement of data protection in the field of legislation.

In 2023 the EU-US Data Privacy Framework came into force and allows, under certain conditions, data transfers to the US (see question 12.2).

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Despite numerous decisions of the ECJ, still quite some open legal questions exist; eg, regarding damages or third country data transfers. The current agreement between the US and the EU for the transfer of personal data is the EU-US Data Privacy Framework. This agreement came into force on July 10, 2023, after the European Commission certified that the US provides an adequate level of data protection and thus made a so-called ‘adequacy decision.’ However, from both a legal and political perspective, there are concerns that the Data Privacy Framework will soon be repealed. Companies that rely on transatlantic data transfers should prepare for possible changes and alternative measures. Last but not least, artificial intelligence poses a challenge for data protection. AI and data protection are often difficult to reconcile, which is why Austria has proposed reforming the GDPR to adopt a risk-based approach similar to that in the AI Act.

12.3 What do you envision the privacy landscape will look like in five years?

The challenges will still be the same: implementing effective technical and organizational measures to secure a reasonable level of security and to keep them up to date.

Ongoing digitalization—and especially artificial intelligence—will bring more challenges as digitalization, and AI brings along a huge flow of data, often big data.

 BELGIUM 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Belgium.

The Belgian legislative and regulatory landscape for privacy, data protection and cybersecurity is comprehensive, and consists of statutory law, constitutional law and European law. These legislative instruments are applied and enforced by the Belgian data protection authority ('DPA'), by the criminal investigation authorities, and by the courts, both directly and upon appeal against decisions of the Belgian data protection authority (in a specialized court of appeals called the Market Court) The Belgian DPA uses its own guidelines, decisions and recommendations when interpreting the laws.

Prior to the entering into force of the EU General Data Protection Regulation ('GDPR'), the Belgian privacy and data protection legislation was set forth in the Act of December 8, 1992 on privacy protection in relation to the processing of personal data ('Data Protection Act'), which was amended to implement the EU Data Protection Directive. The Data Protection Act and the Royal Decrees of February 13, 2001 and December 17, 2003 have been repealed and replaced by the Act of July 30, 2018 on the Protection of Physical Persons towards Treatments of Personal Data ('Privacy Act'). This Act deals with the Belgian substantive aspects of the GDPR, with several specifications and derogations.

Prior to the GDPR, the Belgian enforcement agency was the Belgian Privacy Commission. It monitored compliance, with powers to conduct raids and investigations, but could not impose administrative penalties upon individuals or organizations. The Belgian Privacy Commission, for a variety of reasons, including lack of sufficient resources, had traditionally taken a rather inactive position, only rarely making investigations and decisions. The Belgian Privacy Commission was replaced by the Belgian DPA through the Act of December 3, 2017, which granted it the powers and jurisdiction which the GDPR requires national supervisory authorities to have. Notwithstanding the federal political structure of Belgium, Belgium only has one central DPA.

Another piece of general legislation impacting data protection is the Law of June 13, 2005 on Electronic Communications ('Act on Electronic Communications'), which implemented the ePrivacy Directive 2002/58/EC, with specific privacy rules to the processing of personal data by the telecoms sector.

1.2 What are the primary laws regulating privacy in Belgium? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The GDPR is directly applicable in Belgium and is the principal and primary source for data protection in Belgium. The GDPR covers almost all of the relevant aspects of data privacy.

The Privacy Act is the Belgian national privacy law. Most of the provisions apply to the processing of personal data in the public sector. Only a limited number of principles, issues or opening clauses specifically impact private companies and organizations differently from the provisions of the GDPR.

Other important legislative and regulatory provisions affecting privacy, data protection and cybersecurity are:

- (a) Belgian Constitution ('everyone is entitled to the protection of his or her private and family life');

- (b) Book XII ('Law of the Electronic Economy') of the Code on Economic Law, as adopted by the Act of December 15, 2013, which deals with aspects of information society services and which provides rules on the use of personal data for direct marketing purposes via electronic post (including email, SMS and MMS);
- (c) Books VI and XIV of the Code on Economic Law (market practices and consumer protection, with rules on the use of personal data for direct marketing purposes via telephone, fax and automatic calling machines);
- (d) Act on Electronic Communications; and
- (e) Act of November 28, 2000 on Cybercrime.

Belgium has no sectoral approach to privacy and personal data protection but there are, eg specific rules on the use of surveillance cameras and on the surveillance and monitoring of electronic communications of employees.

All rules on the processing of personal data for marketing purposes are contained in the GDPR. Specific marketing activities, such as direct marketing by email or telephone, are regulated by the Act on Electronic Communications and the Book of the Code on Economic Laws dealing with fair and unfair market practices.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Much of Belgium's self-regulation originates from EU-wide industry initiatives, seeking to ensure compliance with responsible data processing practices, particularly those referenced to in the European Union chapter, including the European Advertising Standards Alliance, the Interactive Advertising Bureau ('IAB') and the European Digital Advertising Alliance. It is worth mentioning that the IAB Transparency & Consent Framework ('TCF'), designed to harmonize the process by which advertisers and publishers obtain user consent for data processing, has itself come under scrutiny, leading to a decision by the litigation chamber of the Belgian Data Protection Authority ('DPA'). The TCF for real time bidding ('RTB') and the Open RTB-Protocol as developed by IAB to self-regulate the instantaneous automated online auctions of user profiles for sale & purchase of advertising space on the internet (for targeted advertising) and its Consent Management Platform ('CMP') for location, age, search history and recent purchases was declared an infringement against the GDPR by the DPA. In its decision of February 2, 2022, the DPA ruled that IAB was a processor of consent, objections and preference choices by data subjects, and the DPA ordered the IAB to take a list of corrective measures and to pay an administrative fine of €250,000. This order of the DPA was challenged before the Market Court and in its judgement of 14 May 2025, the Market Court confirmed the order of the DPA. This is an important reference judgement and equally shows the place for, limitations on, but also high relevance of self-regulation in privacy, particularly for advertising.

1.4 How is privacy law enforced in Belgium? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The GDPR, the Belgian Privacy Act and other laws protecting personal data are enforced by the supervisory Belgian DPA, as well as the courts and the criminal investigation authorities. They can monitor, ask questions, issue orders and fines in case of violations of the data protection laws. In particular, the Economic Inspection Service of the Federal Public Service Economy enforces rules on direct marketing. None of the enforcement agencies are self-regulatory.

The natural enforcement body is the Belgian DPA. The lion's share of enforcement passes through the DPA. Many of the decisions by the litigation chamber of the DPA originate in private complaints of data subjects. Less frequent are private actions initiated through the lodging of a criminal complaint. In such cases, the ensuing criminal investigation (led by an investigation judge) results with a recommendation by the public prosecutor as to whether or not to refer the matter to the criminal court. In contrast, the judicial review of the administrative decisions of the litigation chamber of the DPA rests with the specialist Market Court (see the recent reference ruling in the matter involving IAB, discussed in question 1.3). The most important rulings on privacy law in Belgium are from the Belgian DPA and the Market Court. But other courts in some instances do play a role as well: the extra-ordinary review of the decisions of the Market Court by the Supreme Court—an exceptional example in the field of data protection is in a Facebook decision), the Constitutional Court (exceptionally, such as the so-called 'Informex decision' involving data privacy), the European Court of Human Rights and the Council of State.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Belgium?

See the European Union chapter.

2.2 Does privacy law in Belgium apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law applies outside the country:

- (a) As far as the GDPR is applicable, it applies to companies outside Belgium which:
 - (i) are established in any EU Member State and process personal data as a controller or processor, regardless of whether or not the processing takes place in the EU;
 - (ii) are not established in any Member State but are subject to the laws of a Member State by virtue of public international law; and
 - (iii) are outside the European Union, if they process the personal data of EU residents in relation to the offering of goods or services, or if they monitor the behavior in the European Union of EU residents.
- (b) The Belgian Privacy Act applies to controllers and processors that:
 - (i) process personal data in Belgium (see question 2.1);
 - (ii) do not have an establishment in Belgium, but fall within the scope of the GDPR.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Belgium?

Personal data is legally defined in the GDPR—see the European Union chapter. An identical definition can be found in the Belgian Privacy Act.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

In addition to the specific obligations contained in the GDPR, the Belgian Privacy Act permits private bodies to process special categories of personal data for certain purposes. Some of the most relevant specific Belgian clauses and obligations around sensitive information are:

- (a) The lowering of the age for a child's consent to 13;
- (b) The listing of situations in which processing is deemed to be of substantial public interest, as an exemption to the prohibition on processing the special categories of personal data (principally racial or ethnic origin, political beliefs, religious or philosophical beliefs). The most relevant of these relates to processing by associations which have as their statutory goal the defense and improvement of human rights and fundamental freedoms; and
- (c) Three new obligations for a data controller or processor in relation to the processing of genetic data, biometric data or data concerning health, namely:
 - (i) indicating which categories of persons have access, and explaining their relation to the processing,
 - (ii) maintaining a list of these categories, and
 - (iii) ensuring that the designated persons are subject to a legal or equal contractual obligation to ensure the confidential character of the personal data.

The controller or processor has to take appropriate and specific measures to safeguard the interests of the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

In addition, the approach of the Belgian DPA to data protection impact assessments ('DPIAs') is set out in its February 28, 2018 recommendation, with a Black List of processing operations which always require a DPIA. Some of the most relevant operations on the Black List are:

- (a) processing involving the use of biometric data to uniquely identify individuals in a certain space;
- (b) processing of data collected from a third party in order to make a decision to refuse or to terminate a service contract;
- (c) processing of special categories of personal data for a purpose other than that for which they were originally collected, except where the data subject gives consent, or in particular circumstances;
- (d) medical implants where a data breach can compromise physical health;
- (e) large-scale processing concerning vulnerable people for purposes other than those for which the data were originally collected;
- (f) large scale collections from third parties for the purpose of predicting the economic situation, health, personal preferences, interests, reliability, behavior, location or movements of individuals;
- (g) data of a very personal nature, such as poverty, involvements, domestic and private activities, or location data, being systematically shared between multiple controllers; and
- (h) large-scale processing activities by connected devices ('IoT') (eg, generated by devices, smart toys) or systematic processing through the use of automated processing of certain internet data or metadata, viewing, listening and browsing habits, clicking activity or shopping habits.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for privacy law obligations.

Regulation is dependent on the means of communication:

- (a) The use of electronic means (including email, SMS and MMS) for direct marketing requires the prior authorization of the recipient. This consent has to be specific and freely given on an informed basis (opt-in), except for electronic direct marketing to:
 - (i) legal entities using a non-personal email address (opt-out); and
 - (ii) existing customers about identical or similar products (under specific conditions to be respected and always provided that they can at any time oppose the further use of their electronic contact details for direct marketing purposes) (opt-out).
- (b) A prior consent of the recipient (opt-in) is also required for marketing by fax or through automated calling machines.
- (c) Belgium has a national opt-out register (the 'Robinson List') for marketing by telephone.
- (d) The use of postal services for direct marketing does not require the prior consent of the addressee, provided that an opportunity is offered to opt out. There is an opt-out register for direct marketing by post which is mandatory for members of the Belgian Direct Marketing Association. Non-personalized advertising by post can be stopped through the use of stickers on mailboxes.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

The Act on Electronic Communications implements the EU ePrivacy Directive, pursuant to which the storage of cookies on an end user's device requires prior, specific, informed and freely given unambiguous consent (on the basis of the GDPR standard), unless the cookie is for the sole purpose of carrying out the transmission of a communication, or is strictly necessary to provide the service over the internet.

The Belgian DPA has published recommendations on the use of cookies. Consent cannot be obtained through current browser settings. Consent requires an affirmative action by the user, who must have a chance to review the cookie policy beforehand and who should be given the option to accept or decline the use of each specific category of cookie.

Both the Belgian Institute of Postal Services and Telecommunications and the Belgian DPA have taken enforcement action in relation to cookies. Facebook has been condemned by the Brussels Court of First Instance for having tracked an internet user without knowledge and consent (fine of €250,000 per day with a maximum fine of €100 million). Other enforcement actions taken by the Belgian DPA have given rise to a €15,000 fine for illegal use of cookies on a website.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

In a recommendation of May 2015, the Belgian DPA opposed the use of ‘social plug-ins’ that allow the tracking of the internet traffic and behavior not only of users, but also of internet users with a deactivated account or without any account at all. These recommendations have been enforced through a lawsuit against Facebook.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

Interest-based advertising in Belgium is also governed by the Books VI and XII of the Code on Economic Laws. Search results of a consumer online query must clearly disclose that paid ads or paid advertising result in higher rankings within the search results, at the risk of being challenged for a misleading market practice. Advertising targeting minors based on profiling is banned and targeted advertising based on profiling using special categories of personal data, such as sexual orientation or religious beliefs is also banned, both by the Digital Services Act.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter. There are currently no specific data localization requirements in Belgium.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Belgium? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

9.2 How are personal data breaches regulated in Belgium? What are the requirements for notification and response?

See the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

When a complaint is filed, or an investigation is opened, the DPA will usually start with a fact-finding investigation followed by proceedings on the merits. The decisions can be:

- (a) a settlement proposal;
- (b) a warning and reprimand;
- (c) ordering compliance with the requests;
- (d) the imposition of periodic penalty payments; or
- (e) the imposition of administrative fines.

Transactions can also be proposed. The DPA refers to the methodology of the European Data Protection Board ('EDPB') Guidelines 4/2022 to calculate fines.

The maximum penalty for sending marketing communications in breach of the data protection laws is €10,000 (this amount is a criminal fine and, as such, has to be multiplied by eight). In addition to the administrative sanctions already imposed by the GDPR, fines ranging from €100 to €30,000 for infringements of the Belgian Privacy Act can be imposed.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

The Belgian Privacy Act also introduces a 'cease and desist' procedure to allow a data subject to bring a claim of infringement of data protection obligations before the President of the competent court of first instance. The court can prevent further infringement through an injunction, and can also impose daily penalties and can order the publication of its order. Claims for compensation for damages incurred will necessitate the launch of separate proceedings.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

See the European Union chapter. The Belgian DPA has become very active, making recommendations, opinions and decisions on a near-daily basis. Some of this enforcement relates to advertising. One example is a €15,000 fine of a website operator for use of a privacy statement which was not easily accessible and did not mention the legal basis for the data processing. The DPA referred to the ECJ ruling in Planet49, which determined that effective consent was required for the use of Google Analytics. Blatant security failures can result in high fines. Recent examples include:

- (a) A €200,000 fine on a hospital for failure to conduct a DPIA, to establish an effective information security policy and essential security measures, including training and system log monitoring;
- (b) Fines for GDPR violations at the workplace;
- (c) In the field of dark patterns in cookie consent, the DPA ordered MediaHuis to bring its cookie banners into compliance with the GDPR within 45 days, with a fine of €25,000 per day per website for non-implementation of the changes;
- (d) There are also fining decisions in 2024 for failure to honor data subject rights and non-compliant cookie banners.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Belgium?

In a decision of December 17, 2019, the Belgian DPA fined an operator of a website for legal news which had its privacy statement only available in English, although it was also addressed to a Dutch and French speaking audience.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

As mentioned in the European Union chapter under question 12.1, hot topics include the European Union's AI Act, Data Act and other digital regulation. The AI Act has entered into force and will have direct effect in Belgium as well.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

- (a) Advice issued by the DPA on draft laws covering the use of AI (finding that the rules apply to automated decision-making);
- (b) The September 19, 2024 guideline on AI;
- (c) As from May 31, 2024, representative actions to protect collective interests of consumers have been introduced. This does not lead to full 'class actions', but a more limited collective redress mechanism;
- (d) Also, the EU Data Act has entered into force, with many of its provisions becoming applicable as of September 12, 2025. The purpose of the Data Act is to remove barriers to accessing data.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See questions 11.2 and 11.3.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

See the European Union chapter.

Data breaches caused by insufficient cybersecurity are an ever-increasing source of concern, and trigger potential enforcement by the Belgian DPA, on top of the other concerns and damages inflicted upon private and public entities by cybercrime.

The GDPR is also increasingly being weaponized by parties in discussions and litigation. It remains to be seen when the first class action lawsuits will be filed in connection with data privacy.

The most important upcoming changes are expected in respect of automated decision-making and AI projects.

12.3 What do you envision the privacy landscape will look like in five years?

One can envision substantial progress in terms of clarity achieved as regards the consequences of the use of AI for data privacy, with intensive regulatory and caselaw activity keeping pace with the phenomenal speed of change, as can be witnessed in the healthcare sector. As a smaller country, we can expect Belgium to keep following trend-setting initiatives in neighboring countries or the European Union, as has been a constant feature in privacy over the last decade.

 BULGARIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Bulgaria.

Privacy is regulated on two levels: that of the European Union and that of Bulgaria.

Since May 25, 2018, the primary piece of legislation on the EU level regulating data protection is the General Data Protection Regulation ('GDPR'). This has direct effect in Bulgaria and its rules prevail over any conflicting rules of Bulgarian law.

The right to privacy is set forth in the Constitution of Republic of Bulgaria as a fundamental human right. Its scope goes far beyond the right to personal data protection and also includes the right to personal integrity and non-interference in private life, to non-surveillance, and to secrecy of private communications.

The primary Bulgarian legislative act on data protection is the Personal Data Protection Act ('PDPA'). It sets out derogations and other additional and/or specific data protection rules to the GDPR. The PDPA and its related Rules of the Commission for Personal Data Protection relating to its Activities and Administration ('CPDP Rules') also set out the powers and supervision rules and procedures of the Commission for Personal Data Protection ('CPDP'), which is the Bulgarian data protection supervisory authority.

The PDPA also implements the provisions of the EU Law Enforcement Directive 2016/680, and thus contains special rules on the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of penalties, including the prevention of threats to public order and security.

The Bulgarian Electronic Communications Act ('ECA') provides for the protection of electronic communications networks and services, confidential communications, and the users. It has implemented the ePrivacy Directive (see the European Union chapter).

Certain national sector-specific laws provide for a few sector-specific rules regarding data protection. Such laws include the Bulgarian Consumer Protection Act ('CPA'), which governs commercial communications and includes provisions to protect consumers from misleading advertising and unauthorized data collection, as well as the E-Commerce Act, which applies to online service providers, includes obligations for transparency and aims to achieve lawful processing in digital advertising.

At a secondary legislation level, the CPDP may issue binding rules and instructions regulating in detail the implementation and functioning of legal instruments, such as the technical and organizational measures for personal data protection. Such secondary pieces of legislation must be in conformity with the relevant primary legal act, which, in the case at hand, are the GDPR and PDPA. If they do not conform, these secondary legislative acts may be invalidated as unlawful. As of now, there is only one such piece of secondary legislation in effect, and it relates to the notification of consumers by public electronic service providers in relation to data breaches.

1.2 What are the primary laws regulating privacy in Bulgaria? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary legal acts regulating data protection locally in Bulgaria is the PDPA. It sets out only the local rules on personal data processing under the open and derogating clauses of GDPR. Thus, the principal and core rules on data protection can be found in the GDPR.

Pursuant to the PDPA:

- (a) In case of large-scale processing of personal data or systematic large-scale surveillance of publicly accessible areas, including through video surveillance, controllers must adopt and apply rules for personal data processing, containing:
 - (i) the legal bases and objectives for setting up a monitoring system,
 - (ii) the territorial scope of surveillance and the means of monitoring,
 - (iii) the period of storage of information records and their deletion,
 - (iv) the right of access by the monitored persons,
 - (v) informing the public about the monitoring carried out, as well as restrictions in provision of access to the information to third parties.
- (b) Further, the PDPA prescribes that the processing of personal data for journalistic purposes as well as for academic, artistic or literary expression is lawful when it is performed for the realization of the freedom of expression and the right to information, while respecting privacy of personal life.
 In November 2019, however, the Bulgarian Constitutional Court struck down as unconstitutional the provision of the law which provided for balancing test criteria to be taken into account by controllers when assessing the opposing right of a data subject to personal data protection and the right of other involved subjects to freedom of expression and information (see Decision No 8 of November 15, 2019 under Constitutional Case 4/2019). Thus, at the moment, Bulgarian privacy law does not provide for the implementation of the journalistic exception under Article 85 of the GDPR.
- (c) Another specific rule exists with respect to personal data processing for the purposes of creating a photographic or audiovisual work by filming a person in the course of public activity or at a public place. In this case, the PDPA provides that data subjects cannot enjoy their privacy-related rights further to GDPR, and the regime for data breaches does not apply.

Processing of personal data specifically for marketing purposes is governed by the rules of the GDPR and the ECA. Limited local provisions also apply with respect to direct marketing via email and telephone (see questions 5.3 and 7.1).

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulatory bodies are not common in Bulgaria. As an exception, the National Council for Self-Regulation ('NCSR'), which is a non-profit association created by the Bulgarian Association of Advertisers, the Association of the Advertising Agencies—Bulgaria, and the Association of the Bulgarian Radio and TV Operators to the public benefit, functions as a self-regulatory organization, mainly in the area of advertising, and gives floor to individuals for claims against any noncompliant or unethical pieces of advertising or commercial communication. The NCSR applies the Ethical Code for Advertising and Commercial Communication, which aligns with the International Chamber of Commerce ('ICC') Code of Advertising and Marketing Communication Practice. In addition, the Council

for Electronic Media (the regulator in the field of electronic media), along with Bulgarian National TV, Bulgarian National Radio, and the Association of Bulgarian Radio and TV Operators has drafted and adopted a Code of Conduct to assess and restrict access to harmful programs for children's development. This Code is mandatory for all media service providers and is published on the Council's website.

Notwithstanding, in Bulgaria, self-regulation plays a complementary role in privacy regulation, especially in the context of advertising and marketing practices, and it does not override or replace the statutory requirements stemming from the GDPR, PDPA, or ECA.

1.4 How is privacy law enforced in Bulgaria? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The CPDP is the national data protection supervisory authority. Its powers are set forth in the GDPR and PDPA, and the rules and processes for the exercise of such powers, in the CPDP Rules, respectively. To enforce data protection rules, the CPDP may inspect data controllers and processors, issue and apply mandatory administrative measures, and impose fines and other administrative sanctions. The CPDP exercises its enforcement powers by issuing decisions or other administrative acts which are subject to judicial review at two court instances.

The CPDP enforces the GDPR and national data protection legislation with respect to all data controllers and processors, save for the Bulgarian courts and prosecution and investigation state bodies. The latter are under the jurisdiction of the Inspectorate of the Supreme Judicial Council. When exercising its supervisory functions, the Inspectorate has similar powers to those of the CPDP. The terms and procedures that govern the enforcement powers of the Inspectorate are set out in the Rules of Operation to the Bulgarian Judiciary Act.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Bulgaria?

See the European Union chapter.

2.2 Does privacy law in Bulgaria apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

In accordance with the GDPR, which is directly applicable in the territory of Bulgaria, privacy law does apply to companies established outside Bulgaria. See the European Union chapter.

The PDPA does not include any exceptions or derogations in this respect.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Bulgaria?

Personal data is defined in the GDPR. The PDPA does not supplement or otherwise modify the GDPR definition of personal data in any way.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

In addition to the provisions of the GDPR, Bulgarian laws provide for the following:

- (a) **Children's data and consent:** The processing of personal data of data subjects below the age of 14 on the basis of consent is lawful only if the consent is given by the child's parent or guardian.
- (b) **Copies of personal documents:** The PDPA explicitly restricts cases whereby data controllers and processors may copy an identity document, such as an identity card, driving license or residence document of a data subject—this is permissible only if expressly provided for in a primary legal act.
- (c) **Processing of personal identification credentials:** In Bulgaria, the processing of personal identification numbers ('PIN') of Bulgarian citizens or the processing of the identification numbers of foreigners is subject to enhanced protection. Specific obligations imposed by the PDPA include:
 - (i) an explicit prohibition on the granting of free public access to information containing a PIN, or personal number of a foreigner, unless the law provides otherwise;
 - (ii) controllers providing electronic services must take appropriate technical and organizational measures and not use a person's PIN or personal number as the only means of identifying the user when providing remote access to the respective service.
- (d) **Employee data access requests:** Under Bulgarian employment law, the deadline for employers to respond to employee data access requests with respect to their labor related files, documents and other information is 14 days (in contrast to the period of up to 1 month under the GDPR).

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

Bulgarian data protection legislation does not provide for any specific rules in connection to anonymized, pseudonymized, or de-identified data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

In accordance with the GDPR, the CPDP has published and announced to the European Data Protection Board a revised list of the types of processing operations requiring a prior data protection impact assessment. The list contains eight operations which should be considered by data controllers. They have an obligation to conduct an impact assessment if the personal data processing operations they carry out are among those listed. It should also be noted that the list is non-exhaustive and the CPDP may add or remove qualifying operations from the list at any time.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

The PDPA does not regulate this question. However, the CPDP occasionally issues opinions on the allocation of roles regarding the processing of personal data between companies in common use cases. According to the CPDP, if the service provider's activity involving the processing of personal data is statutorily regulated, there is a high probability, depending on the particular circumstances, that the service provider will qualify as an independent controller.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

Under Bulgarian law, particularly the PDPA, there is no independent or expanded list of privacy notice requirements beyond those provided for in the GDPR.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

Bulgarian legislation does not provide for specific privacy rights which are not already provided for in the GDPR.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

Under Bulgarian law, companies must obtain prior opt-in consent for sending direct marketing via electronic means (eg, email, SMS, automated calls), unless the 'soft opt-in' exception applies (ie, where the individual is an existing customer; the message concerns similar products/services; and the recipient is given a clear and easy opt-out opportunity in every message.).

Additionally, explicit consent is required before placing cookies or tracking technologies used for targeted advertising (explicit prior consent is required to store or access cookies and trackers used for marketing and profiling purposes).

If advertising involves profiling (eg, automated segmentation), and particularly automated decisions, then explicit consent may be required. A data protection impact assessment ('DPIA') would most probably be required.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter.

Certain direct marketing activities, such as email, faxes, text messages and phone calls, are subject to regulation by the ECA, and are, as a general rule, permissible only on the basis of a valid prior and informed consent. However, as an exception to this rule, the ECA allows any entity that has received contact data in relation to the provision of services and/or products to consumers to use that data to contact the customers, including via text messages or emails, for the purposes of marketing and advertising its own similar services and/or products, provided that the company gives each consumer the option to opt out easily from receiving any future messages for any such purpose. For this rule, consumers can be both individuals and legal entities.

For those entities that offer public telephony services, there is a requirement on such entities to obtain the prior explicit consent of subscribers before providing access to their network to third parties to make calls, send text messages and emails for the purposes of direct marketing and advertising. The CPDP may impose an obligation upon the undertakings providing internet access to provide access and to forward emails for free, which will allow end-users with terminated contracts to have access to their messages received from emails.

It is worth noting that the Bulgarian Commission on Consumer Protection keeps a register of the email addresses and telephone numbers of legal entities which have expressly objected to receiving unsolicited commercial communication. Sending unsolicited commercial communication to such contact details of these legal entities is unlawful.

Finally, in any case, direct marketing communication is prohibited when:

- (a) the identity of the sender is disguised or concealed, or
- (b) the provided opt-out address is not valid.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

In Bulgaria, the use of cookies is also regulated by the ECA. The ECA allows the use of cookies, provided that data subjects are duly informed about the use of cookies and have been given the opportunity to refuse the storage of cookies. The providers of information society services must ensure that data subjects are provided with the opportunity, at any time, to check what cookies and information are stored on their devices.

However, these provisions of the ECA have not been tested before the CDPD and the national courts following the GDPR coming into effect. In light of the relevant CJEU case law on the interpretation of the GDPR, installing a cookie manager seeking prior informed consent for each tracking tool that is optional (ie, not necessary) seems to be recognized as an appropriate compliance measure.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

In Bulgaria, targeted and behavioral advertising is regulated primarily through general data protection and electronic communications laws. There are no standalone or advertising-specific statutory rules in Bulgarian national law that specifically or explicitly regulate behavioral or targeted advertising.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7.9 How is advertising to children and minors regulated under privacy law?

In Bulgaria, advertising to children and minors is regulated primarily through the PDPA and the CPA, which impose strict requirements to protect underage individuals. Under the PDPA, parental consent (or legal guardian's consent) is mandatory for processing personal data of children under 14 years old for purposes such as advertising, profiling, or online promotions. Advertisers must implement age verification mechanisms to ensure lawful data use. Additionally, the CPA prohibits misleading, aggressive, or manipulative advertising targeting children, especially content that exploits their credulity, inexperience, or emotional vulnerability. Online tracking and behavioral advertising involving minors require explicit consent from a parent or guardian.

There are also industry-specific restrictions: advertising of alcohol, tobacco, and pharmaceutical products is strictly regulated or prohibited when directed at children. For example, tobacco and alcohol advertising targeting minors is banned outright, and pharmaceutical advertisements must not be aimed at, or use imagery appealing to, children.

Overall, Bulgarian law emphasizes transparency, parental control, and child safety in all advertising practices involving minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

Bulgarian law does not include any special rules in this respect.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Bulgaria? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

9.2 How are personal data breaches regulated in Bulgaria? What are the requirements for notification and response?

See the European Union chapter.

Data breaches related to personal data processing in the context, or for the purposes, of electronic communications are sanctioned further to and otherwise regulated in ECA. There are specific requirements, such as the requirement for electronic communications providers to notify the CPDP within 24 hours of becoming aware of a personal data breach. This is shorter than the 72-hour timeframe mandated by the GDPR. Further, the notification rules and procedures as outlined in EU Regulation 611/2013 apply to personal data breach notifications in this sector, differing from those in the GDPR.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

The CPDP has already imposed fines of:

- (a) BGN 1 million (approx €500,000) on a banking institution for the lack of appropriate technical and organization measures, resulting in the leak of personal data of over 33,000 bank customers;
- (b) BGN 5.1 million (approx €2,550,000) on the Bulgarian National Revenue Agency for a security breach of its software system which led to a leak of financial data of over 6 million persons; and
- (c) BGN 1 million (approx €500,000) on the Bulgarian Posts EAD for failure to implement appropriate technical and organizational measures, resulting in unauthorized access to personal data, including health and financial information.

While the above fines are exceptionally high for the Bulgarian market, in general, throughout the last few years, the fines imposed by the CPDP for individual violations of data privacy tend to range between BGN 10,000 and BGN 60,000 (approx €5,000–30,000), with average of BGN 20,000 (approx €10,000).

Under the Bulgarian Penal Code, some types of information and data security breaches qualify as criminal offenses. Those committing such an offense may be subject to imprisonment for a term of between 1–8 years and a fine of up to BGN 10,000 (approx €5,000). We are not aware of any instances in which such criminal charges have been applied for data breaches or data protection rule breaches.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

The right of data subjects to file a complaint with the CPDP for violation of their personal data is statutorily limited to six months after becoming aware of the violation, and, in any event, not more than two years after the violation was committed. The data subject is not entitled to bring a case for damages, or to challenge data processing activities as being unlawful before the competent court if proceedings are pending before the CPDP with respect to the same claim, or a CPDP decision on the same matter has been appealed and no final and binding court decision has been issued on the matter yet.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The CPDP rarely acts on its own accord in investigating potential non-compliance with the applicable data protection legislation. However, in the event that a data subject (or a state authority) files a complaint/signal/statement of appeal, the Bulgarian DPA always conducts an investigation/check and follows up with appropriate measures.

As a recent development, we have noted that, where a data breach notification is filed by a data controller or processor, the CPDP may, but not always, initiate an inspection of such data controller or processor further to the review of the data breach notification.

We are not aware of any enforcement actions or lawsuits for alleged data breach or privacy non-compliance involving advertising in Bulgaria.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Bulgaria?

Generally, there is public sensitivity to state overreach and surveillance. Bulgarian citizens tend to be less trusting of both public authorities and private companies handling their personal data. Although the awareness among data subjects of data protection and their data protection rights is increasing, a few business organizations consider data protection to be an essential governance obligation and/or as a competitive advantage.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) **Emerging technologies: AI, big data, digital services:** The CPDP has identified the need for DPIAs when implementing technologies like artificial intelligence (‘AI’), Internet of Things (‘IoT’), and big data analytics. These technologies pose risks related to opaque decision-making, potential biases, and privacy invasions. While Bulgaria’s data protection laws align with the GDPR, there are no additional national rules specifically addressing these technologies. The CPDP was actively involved in drafting the bill of law that will ensure the implementation of the Digital Services Act—this bill is still being debated in the Bulgarian Parliament.
- (b) **Whistleblower Protection Act implementation:** In 2023, Bulgaria enacted the Whistleblowing Act, designating the CPDP as the central authority for external whistleblowing. This expanded role includes managing reports of violations and ensuring the protection of whistleblowers. The CPDP has adopted regulations and methodological guidelines to support entities in complying with these new obligations.
- (c) **Cybersecurity:** Bulgaria has not transposed the NIS 2 Directive yet. This set of rules is closely related to data protection and personal data breaches. The relevant bill of law is still under discussion and reading in the Bulgarian Parliament. The law should be enacted in the next few months, and the bill does not provide for a transitional or grace period for compliance. Some companies expected to fall within the scope of the new law have established their cybersecurity compliance plans and are advancing them; however, others are still unfamiliar with the legal framework and their obligations under it.

- (d) **Enforcement trends and sanctions:** The CPDP's enforcement approach remains conservative, with a total of only BGN 74,700 (approx €38,193) in fines imposed in 2024. Notably, only nine cases combined administrative sanctions with corrective measures. The total number of imposed corrective measures for 2024 is 236. The CPDP continues to focus on violations related to data processing principles, legal bases for processing, and security measures.
- (e) **Regulatory focus on specific sectors:** Certain sectors have come under increased scrutiny due to the nature of their data processing activities. These include: CCTV operators; financial institutions; public authorities; political entities; telecommunications and media providers; healthcare providers; courier services providers; direct marketing companies (regarding use of personal data for promotional activities), etc.
For the last couple of years, CPDP inspections of data controllers and processors initiated further to a reported data breach have increased.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Recently, a new chairperson and several new members of the CPDP were appointed. The data protection community in Bulgaria is waiting to see whether the guidance and supervision policy of the Bulgarian data protection authority will stay as it operates now, or whether there will be changes to it.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

See the European Union chapter.

Companies face uncertainty in terms of enforcement. Case law of Bulgarian courts under the GDPR is still limited and relates to the principal rules and clear-cut situations. Concepts such as appropriate technical and organizational measures, balancing of data controller's legitimate interests, data protection by design and by default, etc, have not been reviewed and tested in court yet. In some instances, the adjudications of Bulgarian courts have not been in conformity with the relevant CJEU case law. It is to be seen how court decisions and the entire local enforcement policy in the area of data protection will develop in the coming years. It may reasonably be expected, however, that fines, if and when imposed, will grow in amount.

Other challenges for the private sector include adapting to emerging technologies without clear local guidance. The rapid growth of AI, machine learning, big data, and biometrics introduces complex privacy implications and no detailed national regulation or sectoral guidance.

Another challenge is handling (lawful) cross-border data transfers, especially to third countries outside the EU/EEA/Switzerland.

12.3 What do you envision the privacy landscape will look like in five years?

In five years, the privacy landscape in Bulgaria is likely to become more structured, elaborated and consistently enforced. The area of personal data processing will be significantly penetrated by the use of AI systems and AI models and otherwise driven by digital evolution. Consequently, data protection will be supplemented and aligned with AI governance.

We also expect growing public awareness and responsible data governance to continue. Stronger enforcement by national authorities may contribute to greater compliance.

 CROATIA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Croatia.

Data privacy in Croatia is regulated by statutory law on two levels: that of the European Union and on the national level. On the national level, protection of privacy is also a constitutional category.

Before the EU General Data Protection Regulation ('GDPR') and the Croatian Act on Implementation of the GDPR ('GDPR Implementation Act') entered into force on May 25, 2018 (see question 1.2), the principal piece of legislation which governed protection of data privacy in Croatia was the Act on Protection of Personal Data which was first enacted in 2003 ('Data Protection Act') (now superseded), which established a solid framework for the protection of personal data of Croatian residents.

1.2 What are the primary laws regulating privacy in Croatia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The primary source for data protection in the European Union, and thus in Croatia, is the GDPR. As a binding legislative act—a regulation—it is directly applicable in all EU Member States and does not need to be implemented by the individual Member States. The GDPR covers most of the relevant aspects of data privacy.
- (b) On the other hand, the GDPR contains several opening clauses, allowing EU Member States to enact national privacy rules on certain aspects, which either specify or limit the rights and obligations contained in the GDPR. Croatia has done so with the GDPR Implementation Act. The most important stipulations for the private sector are the following:
 - (i) In relation to the offer of information society services directly to a child, the processing of the personal data of a child is lawful only where the child is at least 16 years old.
 - (ii) The processing of genetic information is forbidden for the purposes of entering into specific agreements in the field of insurance.
 - (iii) The processing of biometric data:
 - in the private sector is permitted only where expressly envisaged by law, or in cases where it is required for the protection of persons, assets, classified data, business secrets or for individual and definite identification of the users of services. The legal ground for the processing of biometric data in the latter case must always be consent; and
 - of employees is permitted only for the purpose of recording working time and for entry/exit records to/from business premises, if stipulated by law or if such processing is an alternative to other means of recording such information. Moreover, this is permitted on condition that employees have given their explicit consent to such processing of data, in line with provisions of GDPR;

The provisions of the GDPR Implementation Act on processing biometric data are applicable to data controllers with the business establishment in Croatia, or which provide services in the territory of Croatia, as well as to public authorities
 - (iv) The processing of personal data by means of video surveillance is regulated in detail.

- (c) In addition, the Croatian Electronic Communications Act and its bylaws set out data retention obligations in relation to the operators as well as, for example, prohibiting the use of automated calling and communication systems without human intervention, facsimile machines or electronic mail, including short messaging system (SMS) and multimedia messaging services (MMS), for the purposes of direct marketing and sale, without the data subject's prior consent.
- (d) There is also sector-specific regulation—for example, in the fields of employment, healthcare, finance and credit. Generally, when it comes to personal data processing for each sector, applicable specific regulations should be taken into account, especially when it comes to determining the legal basis for processing and retention periods.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

While the GDPR and the GDPR Implementation Act are the primary source on protection of personal data, self-regulation may play its role in promoting ethical standards and providing mechanisms on their implementation for its stakeholders, particular in advertising. However, unlike statutory bodies, bodies promoting self-regulation lack binding authority and enforcement mechanisms. For example, the Croatian Association of Communications Agencies ('HURA') encourages best practices in advertising and application of highest standards for its members, however, outside HURA its guidelines are not legally binding and lack enforcement.

1.4 How is privacy law enforced in Croatia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Croatia does not have self-regulatory bodies which enforce the data protection law.

The GDPR, the GDPR Implementation Act, and other laws protecting personal data are primarily enforced by the Croatian Supervisory Authority ('AZOP'), which is authorized to monitor, require the answers to questions, perform supervisions, issue corrective measures and administrative fines. It is not possible to appeal against the decisions issued by AZOP, including decisions related to the issuing of administrative fines. However, it is possible to initiate an administrative dispute before the administrative courts in Croatia.

Certain aspects of data privacy in specific areas are also enforced by other competent authorities. For example, the market regulator for electronic communications—the Croatian Regulatory Authority for Network Industries ('HAKOM')—is tasked with the enforcement of the rules related to unsolicited communications, as well as the use of cookies.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Croatia?

Please see the European Union chapter.

In addition, the additional provisions regarding the processing of biometric data in Croatian GDPR Implementation Act are applicable to data controllers with a business establishment in Croatia or which provide services in the territory of Croatia, as well as to public authorities. See question 1.2.

2.2 Does privacy law in Croatia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy laws apply outside the country. Please see the European Union chapter and question 2.1 above.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Croatia?

Personal data is legally defined in the GDPR—please see the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Please see the European Union chapter. The Croatian GDPR Implementation Act also contains certain country-specific provisions concerning processing of genetic and biometric data (see question 1.2).

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Please see the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Please see the European Union chapter.

In addition, in line with its obligation under the GDPR, AZOP has published a list of the type of processing operations which are subject to the requirement for a data protection impact assessment, which is available on its website.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Please see the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Please see the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Please see the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Please see the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

- (a) Direct marketing: Consent is usually required for direct marketing by automated calling and communication systems without human intervention, fax or electronic mail, including SMS and MMS. Moreover, all electronic mail (including SMS and MMS) sent for the purposes of direct marketing and sales must always have a valid electronic mail address or number to which the recipient may, free of charge, send a request that such communications cease.
In addition, by the Croatian Consumer Protection Act, it is prohibited to make calls and/or send messages by telephone to consumers who have entered their details in the 'do not call' registry. The Registry is held by HAKOM, and it is available online at www.hakom.hr. See further question 7.1.
- (b) The use of cookies, pixels, and similar tracking tools requires prior consent unless they are strictly necessary for the provision of information society services at the express request of the user.
Companies must implement transparent consent mechanisms, such as cookie banners or preference management tools, and maintain records of consent. Withdrawing consent must be easily accessible and effective, ensuring compliance with consumers' rights. Consent must be obtained through a clear affirmative action, granted for each processing purpose (the principle of granularity) and can be withdrawn at any time. See further question 7.2.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Please see the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Please see the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Please see the European Union chapter.

A data protection impact assessment ('DPIA') is required in line with the GDPR at all times when carrying out:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (b) a systematic monitoring of a publicly accessible area on a large scale; or

- (c) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.

In addition, the Croatian Supervisory Authority has published a list of the type of processing operations which are subject to the requirement for a DPIA, which is available on its website and includes:

- (d) Processing of personal data for the purpose of systematic and extensive profiling or automated decision-making, which produces legal effects or significantly affects an individual and/or multiple individuals, or which is used to assist in decisions regarding an individual's access to a service, product, or benefit (eg, processing personal data relating to economic or financial status, health, personal preferences, interests, reliability, behavior, location, or similar);
- (e) Processing of special categories of personal data for the purpose of profiling or automated decision-making;
- (f) Processing of personal data of children for the purpose of profiling, automated decision-making, or for marketing purposes, or for the direct offering of services targeted at them;
- (g) Processing of personal data collected from third parties that are taken into account for decisions related to the conclusion, termination, refusal, or extension of contracts for the provision of services to natural persons;
- (h) Processing of special categories of personal data or personal data relating to criminal convictions and offences on a large scale;
- (i) Processing of personal data involving systematic monitoring of publicly accessible areas on a large scale;
- (j) Use of new technologies or technological solutions for the processing of personal data, or with the potential to process personal data (eg, the application of the 'Internet of Things,' such as smart TVs, smart household appliances, connected toys, 'smart city' systems, smart energy meters, etc), which are used to analyze or predict the economic situation, health, personal preferences or interests, reliability, behavior, location, or movements of natural persons;
- (k) Processing of biometric data where at least one additional criterion from the Guidelines on Data Protection Impact Assessment (WP 248 rev 01) is met, which is used to assess whether certain processing operations are likely to result in a high risk to the rights and freedoms of data subjects;
- (l) Processing of genetic data where at least one additional criterion from the Guidelines on Data Protection Impact Assessment (WP 248 rev 01) is met, which is used to assess whether certain processing operations are likely to result in a high risk to the rights and freedoms of data subjects;
- (m) Processing of personal data involving the linking, comparison, or matching of data from multiple sources;
- (n) Processing of personal data that involves tracking an individual's location or behavior in cases of systematic processing of communication metadata generated through the use of telephones, the internet, or other communication channels, such as GSM, GPS, Wi-Fi tracking, or processing of location data;
- (o) Processing of personal data using devices and technologies where an incidental event could endanger the health of an individual or multiple individuals; and
- (p) Processing of employees' personal data through the use of applications or systems for monitoring (eg, processing personal data for tracking work, movements, communications, or similar).

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Please see the European Union chapter.

In addition, under the Croatian Electronic Communications Act, use of automated calling and communications systems without human intervention, facsimile machines or electronic mail, including SMS messages and MMS messages, for the purposes of direct marketing and sale is only allowed in respect of subscribers, or users who have given their prior consent. Consent is not required for such communications made to legal persons; however, this exception is only applicable if such communications do not involve personal data (ie, if you cannot identify an individual either directly or indirectly).

There is also an exception for a trader (which can be a natural or a legal person) which may use email addresses obtained from its customers for the purpose of sale of products or services for direct marketing and sale of its own similar products or services, provided that customers are, clearly and distinctly, given the opportunity to object, free of charge and in an easy manner, to such use, both when the electronic mail address was collected and on the occasion of receiving any electronic message in cases where the customer has not initially refused such use of the information.

All electronic mails (including SMS and MMS) sent for the purposes of direct marketing and sales must correctly display and not conceal the identity of the person on whose behalf the electronic mail or message is sent, and they should always have a valid electronic mail address or number to which the recipient may, free of charge, send a request that such communications cease.

HAKOM has also established a 'do not call' registry, in which the subscribers can register their telephone numbers in case that do not wish to receive unsolicited communications. Note that the 'do not call' registry applies only to consumers. A 'consumer' is defined by the Croatian Consumer Protection Act as any natural person who enters a legal transaction or operates on the market outside of its trade, business, craft, or professional activity.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Please see the European Union chapter.

Regarding cookies, in November 2019, HAKOM issued a decision in which it confirmed the position taken by the European Court of Justice in the Planet49 case. Namely, that an effective consent requires an unambiguous action of confirmation, such as actively clicking a box affirming consent on a website. In contrast, a box that is pre-ticked, or the inactivity of the user cannot establish effective consent in the sense of the GDPR. Accordingly, cookie banners which seek to establish consent simply through a user continuing surfing on a website are not admissible.

This approach has been confirmed in the Electronic Communication Act, whereby cookies and tracking technologies require prior explicit user consent for all non-essential cookies and clear information on data processing purposes. Companies must implement transparent consent mechanisms, such as cookie banners or preference management tools, and maintain records of consent. Withdrawing consent must be easily accessible and effective and available at the mere website ensuring compliance with consumers' rights. Consent must be obtained through a clear affirmative action, granted for each processing purpose (the principle of granularity) and can be withdrawn at any time.

7.3 How are loyalty programs and promotions regulated under privacy law?

Please see the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

Please see the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Please see the European Union chapter.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Please see the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

Please see the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

Please see the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

Please see the European Union chapter.

In addition, the Croatian GDPR Implementation Act envisages, in relation to the offer of information society services directly to a child, that the processing of the personal data of a child is lawful only where the child is at least 16 years old.

Also, processing of personal data of children for the purpose of profiling, automated decision-making, or for marketing purposes, or for the direct offering of services targeted at them, is listed by the Croatian Supervisory Authority in its published list of the type of processing operations which require a DPIA.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Please see the European Union chapter.

In addition, the following are listed by AZOP in its published list of the type of processing operations which are subject to the requirement for a DPIA:

- (a) Processing of personal data for the purpose of systematic and extensive profiling or automated decision-making, which produces legal effects or significantly affects an individual and/or multiple individuals, or which is used to assist in decisions regarding an individual's access to a service, product, or benefit (eg, processing personal data relating to economic or financial status, health, personal preferences, interests, reliability, behavior, location, or similar); and

- (b) Use of new technologies or technological solutions for the processing of personal data, or with the potential to process personal data (eg, the application of the 'Internet of Things,' such as smart TVs, smart household appliances, connected toys, 'smart city' systems, smart energy meters, etc), which are used to analyze or predict the economic situation, health, personal preferences or interests, reliability, behavior, location, or movements of natural persons.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Please see the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Please see the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Croatia? Are there minimum standards? Does this differ by sector or size of the entity?

Please see the European Union chapter.

In addition, AZOP has published on its website technical and organizational measures for securing personal data, which may include, inter alia:

(a) Technical measures:

- (i) setting passwords and access rights to data, programs and equipment.
- (ii) regular upgrading of the operating system and computer programs.
- (iii) installing an antivirus program on devices.
- (iv) data backups (backup).
- (v) installing a firewall.
- (vi) protection of access to the network infrastructure.
- (vii) encryption of data and portable devices.
- (viii) protection of data stored in paper form.
- (ix) physical protection against unauthorized access.
- (x) internet router protection against unauthorized access.
- (xi) protection of access to data from remote locations against unauthorized access.
- (xii) access to equipment and programs via chip cards.

(b) Organizational measures (ie internal acts and documents):

- (i) Information Security Bylaw, which prescribes technical protection measures that are applied to protect data from unauthorized access in a business entity;

- (ii) Bylaws regulating the processing of personal data, prescribing who processes personal data, for what purpose, the legal basis for processing, the scope of personal data that is processed, who has the right to access and process personal data, how long the data is kept, etc;
- (iii) contractual clauses within an employment contract may define the collections of personal data that the employee will process and what rights they will have for the processing of these storage systems (or databases);
- (iv) contractual clauses within a business co-operation agreement defining the collections of personal data that are the subject of the contract, the rights and obligations of each of the contracting parties regarding the processing of personal data, and which technical protection measures each of the parties undertakes to protect the data storage systems (databases); and
- (v) declarations of confidentiality stipulating that an employee of a business entity or an external collaborator gives a written statement that they will process personal data in accordance with the legal provisions on the protection of personal data, as well as implementing appropriate protection measures on it and not abusing it or giving it to unauthorized third parties.

9.2 How are personal data breaches regulated in Croatia? What are the requirements for notification and response?

Please see the European Union chapter.

AZOP has published on its website a template of the form for data breach notifications.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Please see the European Union chapter.

In addition, further to the GDPR Implementation Act, authorized officials of AZOP can conduct announced or unannounced inspections independently, and, in certain cases, with the participation of representatives of a representative official from a supervisory body within the European Union.

Authorized persons may seal storage systems or equipment for a maximum of 15 days during inspection/surveillance if there is a risk of destruction or alteration of evidence. If, during the inspection/supervision, information is obtained or objects are found that indicate that a criminal offence has occurred, for which *ex officio* prosecution is envisaged, the authorized officials will inform the competent police station or the state attorney as soon as possible.

10.2 Do consumers have a private right of action? What remedies are available to them?

Please see the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Please see the European Union chapter.

In addition, in September 2023, AZOP announced administrative fines related to cookies for the first time in Croatia. Namely, AZOP imposed two administrative fines on data controllers in the gambling and betting industry, in the amount of €20,000 and €30,000, due, in both cases, to three established violations of the GDPR. The data controllers:

- (a) collected and processed personal data of data subjects/website visitors via cookies without a legal basis,
 - (b) did not adequately provide information to the data subjects to enable them to give and/or withdraw informed and voluntary consent; and
 - (c) did not adequately inform data subjects (website visitors) about the processing of personal data through cookies,
- thereby violating provisions of GDPR.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Croatia?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

It will remain to see the interesting interplay between the regulations on cybersecurity, artificial intelligence and data protection.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Apart from the entering into force of the AI Act and the Data Act on the EU level, the Croatian Electronic Communications Act has been updated to align with the EU's Privacy and Electronic Communications Directive. These amendments reinforce rules on cookies and tracking technologies used in advertising, requiring explicit user consent for non-essential cookies and clear information on data processing purposes. Fines for violations, such as unauthorized use of cookies in online advertising, can reach up to €130,000. HAKOM oversees enforcement in this sector.

In addition, in order to strengthen provisions on direct marketing, the Croatian Consumer Protection Act has been amended to prohibit the disclosure of consumer data without consent and imposing fines up to €13,000 for breaches such as unsolicited marketing communications. These changes aim to enhance consumer protection in advertising practices, aligning with GDPR consent requirement.

Following the NIS2 Directive, the Croatian Parliament has adopted the Cybersecurity Act. This introduces stricter cybersecurity requirements for essential and important entities from different/broader sectors. The Cybersecurity Act has further prescribed the obligations for data breach notifications and security measures that complement GDPR obligations, indirectly affecting advertising platforms that process personal data.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The Croatian Cybersecurity Act which has transposed the NIS2 Directive, has broadened the scope of entities subject to cybersecurity obligations, by categorizing them as essential entities (eg, critical infrastructure operators in sectors like energy, transport, banking, and healthcare) and important entities (eg, certain digital service providers and other organizations with significant impact).

12.3 What do you envision the privacy landscape will look like in five years?

It appears that the GDPR will remain the cornerstone of data protection with even more strict enforcement by AZOP. The interesting interplay between the regulations on cybersecurity, artificial intelligence and data protection remains to be seen.

CYPRUS

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Cyprus.

Privacy rights are regulated through various mechanisms in Cyprus. Specifically, privacy law is regulated through legislation of the European Union and through domestic legislation, as well as the Cypriot Constitution. At present, the main source of privacy legislation is the EU General Data Protection Regulation ('GDPR'), which came into force in May 2018 and is directly applicable to all EU Member States. As a regulation, the GDPR is directly enforceable and applicable across the EU Member States.

Law 125(I)/2018 is the national law on data protection in Cyprus, providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data.

The national competent authority which is responsible for data protection is the Office of the Commissioner for Personal Data Protection (the 'Commissioner'), which has the power to monitor data protection and issue major guidelines.

The Courts of the Republic of Cyprus are responsible for the interpretation of the national law.

1.2 What are the primary laws regulating privacy in Cyprus? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) As mentioned above, the GDPR is the primary source of legislation on privacy.
- (b) In addition, Cyprus has adopted national legislation (Law 125(I)/2018) for the effective implementation of certain provisions of the GDPR and to increase its effectiveness. The GDPR contains several opening clauses which allow EU Member States room to regulate stricter or broader significant rights and obligations. The most important additions effected by Law 125(I)/2018, when compared to the GDPR, are the following:
 - (i) The processing of genetic and biometric data for purposes of health and life insurance is prohibited, except where the data subject gives consent.
 - (ii) Certain infringements of privacy law rights are specified to be criminal offenses, and penalties are set out for these (see questions 9.2 and 10.1).
- (c) Further Cyprus has enacted Law 44(I)/2019 'on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties and their transmission', which is another main piece of legislation. This law specifically regulates the processing of information by the Cypriot Police, the Cyprus Customs and Excise Department, the Unit for Combating Money Laundering and the Tax Department.
- (d) In the context of advertising and marketing, the key legislation is the Electronic Communications and Mail Services Law (Law 112(I)/2004), which regulates privacy law and, amongst other matters, direct marketing messages through electronic communications.
- (e) Finally, private life and respect for the secrecy of correspondence is a fundamental right in Cyprus embedded in its Constitution. These are now to be read in light of the GDPR provisions.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Cyprus does not have any self-regulatory bodies which enforce privacy law.

1.4 How is privacy law enforced in Cyprus? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The GDPR and other privacy laws are enforced by the Commissioner, which is not only responsible for the monitoring of the legislation and the imposition of fines in case of violation of data protection laws, but also answers questions and issues guidelines relating to the protection of privacy rights. In certain cases, the Commissioner assists organizations and businesses through prior consultation.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Cyprus?

See the European Union chapter.

2.2 Does privacy law in Cyprus apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law applies to companies outside the country. See the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Cyprus?

Personal data is legally defined in the GDPR (see the European Union chapter).

In addition, pursuant to Law 125(I)/2018 and Law 44(I)/2019, ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Apart from the specific obligations regarding information under the GDPR, Law 44(I)/2019 specifies the circumstances in which the processing of certain personal data is permitted, namely data which refers to the racial or ethnic origin, political beliefs, religious or philosophical beliefs or participation in trade unions, as well as the processing of genetic data or biometric data for the exclusive identification of a natural person, or data which concern health or sex life or sexual orientation. This is permitted only when it is strictly necessary, without prejudice to appropriate safeguards for the data subject’s rights and freedoms, and provided that:

- (a) it is permitted by EU law or relevant legislation;
- (b) it is necessary to protect vital interests of the data subject or other natural person, or
- (c) such processing concerns data that has been publicly disclosed by the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

- 6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?**

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

- 7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?**

Under Law 112(I)/2004, there are some direct marketing activities, such as emails, telefaxes, text messages and phone calls, which are, as a general rule, only permissible on the basis of a valid and informed prior consent that has been given by subscribers/users regarding the specific means of direct marketing.

Law 112(I)/2004 is also relevant regarding the cookie policy of websites, as to which see also the European Union chapter.

- 7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?**

See the European Union chapter and see question 7.1 above.

- 7.3 How are loyalty programs and promotions regulated under privacy law?**

See the European Union chapter.

- 7.4 How is social media and influencer marketing regulated under privacy law?**

See the European Union chapter.

- 7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

See the European Union chapter.

- 7.6 How are digital identity resolution and clean room technologies regulated under privacy law?**

See the European Union chapter.

- 7.7 How is location-based advertising regulated under privacy law?**

See the European Union chapter.

- 7.8 How are data brokers defined and regulated under privacy law?**

See the European Union chapter.

- 7.9 How is advertising to children and minors regulated under privacy law?**

Processing personal data of children under 14 for information society services requires verifiable parental consent. See the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

Additionally, there are restrictions in cases where transmission of specific categories of personal data to a third state or to an international organization takes place:

- (a) According to Law 125(I)/2018, where transmission is to take place according to Article 46 of the GDPR, the controller or processor must inform the Commissioner of its intention prior to the transmission of such data. The Commissioner is able, for fundamental public policy reasons, to impose on the controller or the processor restrictions on the transmission of personal data.
- (b) In addition, Law 125(I)/2018 stipulates that the transmission of specific categories of personal data, on the basis of derogations for special situations according to Article 49 of the GDPR, requires an impact assessment to be carried out and prior consultation by the Commissioner prior to the transfer. The Commissioner has the power to impose explicit restrictions on the transmission of specific categories of data to the controller or the processor.
- (c) Law 44(I)/2019 is also relevant, whereby any transmission of personal data to a third country or international organization, may only take place if the following requirements are fulfilled:
 - (i) the transmission is vital for the purposes of prevention, investigation, detection or prosecution of criminal offenses, protection of public order and security, freezing or confiscating illicit proceeds or other related assets or for executing criminal fines;
 - (ii) personal data is to be transmitted to a controller in a third country or international organization which is a competent authority,
 - (iii) where personal data is transmitted or made available by another Member State, that Member State has previously given its approval for the transmission in accordance with its national law;
 - (iv) the European Commission has made an adequacy decision or, in the absence of such a decision, sufficient guarantees have been afforded; and
 - (v) in the event of a further transfer to another third country or international organization, the competent authority which carried out the original transfer or another competent authority in the same Member State shall allow the further transfer, taking due account of all relevant factors, including the seriousness of the criminal offense.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Cyprus? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

9.2 How are personal data breaches regulated in Cyprus? What are the requirements for notification and response?

See the European Union chapter.

It should be further noted that Cyprus has made use of the opening clauses to the GDPR (see question 1.2(b)) to constitute certain infringements of privacy law rights as criminal offenses, and set out penalties for these (see question 10.1). In particular:

- (a) when a controller or a processor provides false, inaccurate, incomplete or misleading information to the Commissioner, or fails to cooperate with the Commissioner, or prevents the data protection officer from performing their tasks, particularly those relating to the cooperation with the Commissioner; or
- (b) when a controller does not notify the Commissioner of a personal data breach, or does not carry out an impact assessment.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter in respect to the GDPR.

Apart from the GDPR, Law 125(I)/2018 renders several breaches of privacy law to be criminal offences (see question 9.2). If a person is convicted of committing any of these offenses, they may be subject to imprisonment not exceeding one, three, or five years, depending upon the seriousness of the infringement, or a fine of up to €10,000, €30,000, or €50,000. Further, according to Law 44(I)/2019, the Commissioner has the power to impose on the competent authority acting as controller an administrative fine in case of infringement of up to €100,000.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

Apart from making complaints to the Commissioner, data subjects also have a private right of action in the Administrative Court against the controller or processor if they consider that their privacy rights have been violated. In addition to this, data subjects have the right to delegate their claim to non-profit organizations or associations to exercise their rights on their behalf.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

See the European Union chapter.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Cyprus?

See the European Union chapter.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Technology's presence in every aspect of advertising is well established today. Therefore, the appropriate technical and organizational measures required by the GDPR should be implemented. Data processing should be based on one of the legal bases of the GDPR and meet the principles related to the processing of personal data. The minimization of personal data processed, as well as the principle of transparency should be applied in accordance with the Regulation, regardless of the technology used for advertising purposes.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

Undoubtedly, the most important trigger for changes to the privacy landscape has been the rapid technological development over recent years, and the EU legal framework (GDPR) that seeks to fill the gaps between the national legislation and technological development.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies in recent years have faced countless uncertainties due to the influence of digital data. The European Union has sought to revolutionize the status quo of privacy law, and this has resulted in the GDPR, whereby the previous lack of uniformity has been transformed into a more precise and certain approach by the EU Member States.

12.3 What do you envision the privacy landscape will look like in five years?

In five years' time, it is very likely that the scope of the GDPR will become clearer due to the decisions that will be issued by the European supervisory authorities. The evolution of technology and artificial intelligence in particular may bring about rapid changes in the field of data protection. Thus, the requirement for a data protection impact assessment prior to any data processing and full compliance with the principles of the GDPR will be considered very important in order to further safeguard the rights and freedoms of individuals.

CZECH REPUBLIC

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in the Czech Republic.

Data privacy and personal data protection is regulated in particular by constitutional law, applicable Czech legal regulation and European law.

The constitutional basis of the right to privacy is stipulated in the Declaration of the Fundamental Rights and Freedoms of the Czech Republic ('Declaration') and is generally regulated by the Czech Civil Code ('Civil Code').

The Declaration provides that the integrity of persons and their privacy is guaranteed and may be restricted only in cases provided for by law. This principle is reflected in the Civil Code, which states that no one may invade the privacy of another unless for a lawful reason. That lawful reason will be, first and foremost, the relevant permission given by the person. However, even such permission cannot allow an interference which would be contrary to the legitimate interests of a person in the protection of their personality.

The GDPR is directly applicable in all EU Member States without the need for implementation into national law. The GDPR thus unified data protection legislation across the entire European Union, thereby facilitating the free movement of personal data across Member States. In the Czech legal system, the GDPR replaced local regulation, which had to be amended; therefore a new Act on Personal Data Processing ('APDP') was adopted in April 2019.

The applicable legal regulation is interpreted by the Czech and European case law; the statements, resolutions, opinions and guidelines of the Czech supervisory authority for data protection, the Data Protection Authority ('DPA'); and the recommendations and guidelines of the European Data Protection Board ('EDPB').

1.2 What are the primary laws regulating privacy in the Czech Republic? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The constitutional basis of privacy and personal data protection is stipulated in the Declaration, complemented by ETS 108, Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union.

The protection of the right to privacy and image of the individual persons is regulated by the Czech Civil Code.

Personal data protection is regulated comprehensively by the GDPR and the APDP. The GDPR provides for majority of legal obligations. The APDP implemented the Criminal Law Directive and adapted the GDPR to ensure that national legislation complies with these rules and, where appropriate, set more specific rules in some areas where the GDPR directly permits Member States to do so.

The APDP provides for the following:

- (a) personal data processing pursuant to the GDPR;
- (b) personal data processing by the competent authorities for the purpose of the prevention, investigation or detection of criminal offences, prosecution of criminal offences, execution of criminal penalties, and protective measures, ensuring the security of the Czech Republic and ensuring public policy and national security, including search for persons and objects;

- (c) personal data processing in ensuring the defense and security interests of the Czech Republic;
- (d) other processing of personal data that form or are intended to form part of a filing system or that are processed wholly or partly by automated means, other than personal data processing by a natural person in the course of a purely personal or household activity; and
- (e) the status and powers of the DPA.

The APDP has not made use of the possibility of amending general GDPR rules in many cases. However, the APDP introduces exemptions from the obligation to assess the impact of processing on the protection of personal data, exceptions from the obligation to notify data subjects, and adjusts the processing of personal data for journalistic, academic, artistic or literary purposes.

The implementation of GDPR rules has entailed the amendment of many other regulations in various fields of business activities.

The area of B2C relationships in advertising is mainly implemented by the Electronic Communications Act ('ECA') and the Act on Selected Services of the Information Society ('SSIS').

The rules on the use of cookies and telephone marketing are regulated by the ECA.

The rules for sending commercial communications (advertisements sent by electronic means) are regulated by the SSIS.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation does not play a significant role in Czech national regulation of privacy and advertising.

There are no self-regulatory bodies specializing in privacy law. The primary advertising self-regulatory body in the Czech Republic is the Czech Advertising Standards Council ('CASC') which is a member of European Advertising Standards Alliance. The CASC brings together clients, agencies and the media with the aim of ensuring that advertising is honest, legal, decent and truthful, in particular by enforcing its Code of Advertising Practice ('Advertising Code').

According to the Advertising Code, an advertisement must not depict any living persons or make any reference to any living persons unless such persons have expressly consented in advance. Advertisers must also be careful not to offend, religiously or otherwise, persons associated in any way associated with deceased persons depicted in the advertisement or deceased persons to whom any advertisement refers. In relation to politicians and public authorities in general, the Advertising Code is stricter. Advertising must not use public authority holders (eg, politicians, or representatives of professional medical and other societies) for advertising purposes, even if they agree to appear in the advertisement, and whether they get paid or not.

The CASC does not have official authority to impose obligations or fines and its decisions are only recommendations. However, the CASC does have authority to give expert opinions on the practical application of the Regulation of Advertising Act and it also provides preliminary opinions to advertisers before launching a campaign.

There is also a specialized self-regulatory initiative of influencer marketing, Fer Influencer, which publishes its own code, and influencers can become members to show their commitment to fair practices. Complaints can be made with a committee for self-regulation of internet content, which operates as a part of SPIR, an organization aimed at development of the Czech online market. No official authority is held by any of these self-regulatory bodies.

1.4 How is privacy law enforced in the Czech Republic? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Czech Republic does not have any self-regulatory bodies which enforce privacy law.

The obligations stipulated by the GDPR and the APDP or other applicable legal regulation are enforced by the DPA and, in cases where the decision of the DPA is appealed, by the Czech courts.

The DPA is vested with additional powers related to special issues and anchored in special laws. The basic procedural Acts are the Supervisory Procedure Act and the Administrative Code.

The DPA has a role in supervising electronic communications, as provided by the ECA. Supervision of bulk commercial communication is regulated by the SSIS, and non-compliance is punishable by fines. Transborder supervisory cooperation is provided by EC Regulation 2006/2004 on consumer protection cooperation. The role given to the DPA in advertising by the Regulation of Advertising Act is similar, namely supervision of compliance of any unsolicited advertising disseminated with help of electronic means.

The Basic Registers Act provides that the DPA should generate source identifiers of physical persons and item-related identifiers of natural persons, and maintain lists thereof, and ensure transfers of a natural person's item-related identifier within one administrative dossier to item-related identifier of this physical person under another dossier on the basis of a legal request.

In the public sector, unauthorized processing of information stored on biometric data carriers is punishable by penalties provided by the Travel Documents Act; and minor offenses constituting further non-compatible processing of data, breach of confidentiality and unauthorized disclosure are set out in the Register of Population Act and the Conflict of Interests Act.

Privacy rights stipulated in the Civil Code or the right to compensation under the GDPR can be enforced individually by filing an action with a Czech court. All courts must provide protection of the basic right to privacy in any case brought before the court. Group actions can be filed if the case is related to consumer protection and other conditions are met.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in the Czech Republic?

See the European Union chapter.

Privacy law (under the Civil Code and related legislation) applies to all companies if Czech law applies.

2.2 Does privacy law in the Czech Republic apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

See the European Union chapter.

Basic privacy law (under the Civil Code) applies to anyone (including foreign companies) if Czech law applies according to international law principles.

Privacy law in an commercial and advertising context applies to companies outside the Czech Republic which undertake business in the territory of the Czech Republic. It follows from Czech law that persons who do not reside in the territory of the Czech Republic or legal persons who do not have their

registered office in the territory of the Czech Republic may operate a trade in the territory of the Czech Republic under the same conditions and to the same extent as a Czech person, unless specified, or a special law provides, otherwise.

In practice, this means that a foreign person (legal or natural) may start business in the Czech Republic on the date of its registration (or registration of its branch office or company) in the Trade Licensing Register or Commercial Register, and to the extent registered in the respective register (with certain exceptions).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in the Czech Republic?

See the European Union chapter.

Whilst the definition of ‘personal data’ stipulated in the GDPR has not been changed in the APDP, the interpretation and the scope of ‘personal data’ in the Czech Republic may be interpreted more extensively in practice due to case law (see, eg, the ruling of the CJEU in the *Nowak* case, where it held that written answers submitted by a candidate in a professional examination and any comments made by an examiner with respect to those answers constitute personal data).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

Relevant case-law emphasizes a proper distinction of anonymized data (ie, subject cannot be identified) with regard to all information available—not only to the controller (entity carrying out the anonymization) but also the recipient of such anonymized data. Czech case-law has assessed the possibility of identifying a person based on a case-file number with a positive outcome. The same approach applies to the distinction between anonymized and pseudonymized data, ie, whether the recipient of such data is able to identify a person based on all information available to them.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

In addition, it is explicitly stipulated in the APDP that a child has capacity to grant consent to the processing of personal data in relation to the offer of information society services on reaching 15 years of age.

Information society services are subject to the SSIS. An ‘information society service’ is defined in the SSIS as any service provided by electronic means on individual demand of the user filed by electronic

means, usually provided for a certain fee; a service is provided by electronic means if it is sent via electronic communications network and picked up by the user from the electronic device for data storage.

The providers of information society services are, nevertheless, not obliged to supervise the content of information transmitted or stored by them, or to actively seek facts or circumstances indicating the unlawful content of the information.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

In addition, entrepreneurs should bear in mind that the correct determination of the role of their company in a specific contractual relationship (controller/processor) and with respect to specific processing is essential to determine the risks related to liability in case of a data security breach or other violations under the GDPR.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

Beyond lawful bases stipulated in the GDPR, under the APDP, personal data may also be processed if it serves in an appropriate manner for journalistic purposes or for the purposes of academic, artistic or literary expression. Furthermore, the APDP also stipulates conditions of processing of personal data for scientific or historical research purposes or for statistical purposes.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

When processing personal data for advertising purposes, the SSIS and ECA are applicable, as well as non-binding guidance from the DPA.

In particular, the following points are strongly emphasized by the DPA:

- (a) consent for direct marketing (eg, email, SMS);
- (b) consent for behavioral advertising (cookies, etc); and
- (c) legitimate interest for advertising.

Consent provided must be always given freely, under no pressure, and unambiguously. Most importantly, pre-ticked boxes, bundled consents, or unclear wording is prohibited and can lead to fines. Also, data subjects must understand what they are agreeing to, how their personal data will be processed, and what channels will be used for marketing purposes. Opt-out options must be provided in every message and proof of consent must be kept at all times.

For technologies such as cookies, tracking pixels, and device fingerprinting, consent is also required before data is processed unless it's strictly necessary (as per the ePrivacy Directive and Czech law).

Users must have the ability to:

- (i) accept or reject non-essential cookies;
- (ii) access detailed cookie categories; and
- (iii) change their consent settings later.

Legitimate interest (as mentioned in the GDPR) can be used only in limited advertising cases, typically for non-intrusive direct marketing (eg, promoting similar products to existing customers). When ascertaining the legitimate interest, several tests (purpose test, necessity test, and balancing test) should be conducted. In the Czech Republic, the DPA tends to favor consent over legitimate interest for online tracking and profiling.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

In an advertising context, it is important to emphasize the right to withdraw consent (and to be able to do so easily) and the obligation to obtain consent before using cookies (or other technology used for tracking, storing data or gaining access to data stored in a device).

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

In addition:

- (a) **Electronically disseminated commercial communications** are specifically governed under the SSIS. One may only use an electronic contact (eg, email) for the purpose of disseminating commercial communications electronically if users have granted their prior consent.

However, if a natural or legal person obtains electronic contact details from customers in relation to selling products or services to them, such person may use these electronic contact details for the purpose of disseminating commercial communications related to its own similar products or services (the ‘customer exception’). This is possible on condition that customers have a clear opportunity to easily withdraw consent to such use of their electronic contact, free of charge or on the account of such natural or legal person. This possibility must be present in each individual message, if the customer did not originally decline such use.

Along with the above conditions, natural or legal persons intending to disseminate commercial communications via electronic mail have to ensure that each message:

- (i) is clearly labelled as commercial communication,
- (ii) does not hide or conceal the identity of the sender on whose behalf the communication takes place, and
- (iii) contains a valid address to which the addressee can directly and effectively send the information that they do not wish commercial information to be sent to them by the sender anymore.

The agenda of (unsolicited) commercial communications is governed by the DPA, and the DPA regularly undertakes inspections in this field. In 2023, a penalty of nearly CZK 8 million (approx €322,000) was imposed for repetitive unsolicited email marketing conducted without the recipient’s consent.

The DPA has issued a comprehensive FAQ on its website regarding commercial communication.

- (b) **Subscriber lists/directories:** Pursuant to the ECA, any person who collects personal data of users in order to issue a subscriber list (directory) for the purpose of retrieving detailed contact information about a person on the basis of that person's name or certain other personal or identifying data, must:
- (i) inform the subscribers concerned, prior to the inclusion of their data in the list, of the purpose of the printed or electronic subscriber list which will be available to the public directly or through enquiry services and of other possibilities of use based on the search functions contained in the electronic versions of the list; and
 - (ii) obtain the prior consent of subscribers to the publication of their personal and identifying data, and ensure that subscribers have the opportunity to determine which personal data is to be included in the public list. Subscribers must have the opportunity to verify such data and request its correction and removal. At the same time, subscribers or users must be given the opportunity to indicate whether or not they are willing to be contacted for marketing purposes.

There must be no charge for being listed in the public list of subscribers, for verifying, correcting and removing personal data from the list or for indicating whether or not a subscriber or user is willing to be contacted for marketing purposes.

Only personal data (name, surname, pseudonym, home address, telephone number, email address and, where applicable, address of the registered office of the person's business) and identification data (business name or trade name, registered office or head office, address and telephone number of the place of business and email address) may be part of the subscriber list; however, other data of subscribers may also be published in the list if so agreed by contract with them. Personal and identification data of subscribers who have not consented to their publication may not be published.

The random generation of telephone numbers is also deemed to constitute a subscriber list, as well as telephone numbers without other identifying information or a list that includes telephone numbers or personal or identifying information of subscribers who have not indicated that they wish to be contacted for marketing purposes.

It is prohibited:

- to offer marketing advertising or other similar means of offering goods or services through electronic communications networks or services to subscribers or users who have not indicated in the public list specified above that they wish to be contacted for marketing purposes;
 - to use subscriber lists, or an electronic communications network or service for the purpose of direct marketing by means of automated dialing devices, fax machines or email, unless the subscriber or user concerned has given prior consent;
 - for an undertaking providing a service of enquiries on subscribers' numbers or other similar data to provide subscriber data which is not contained in the public directory;
- and a provider of publicly available electronic communications services whose commercial interests are harmed by a breach of these obligations is entitled to seek judicial protection on behalf of its subscribers whose rights have been harmed by such conduct (or subscribers can pursue their claims in court on their own behalf).

The Czech Telecommunication Office has, in cooperation with the DPA, issued an interpretative notice on this matter, with quite an extensive FAQ section, that may serve as a guidance.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

In the Czech Republic, companies must follow strict rules when they engage vendors and third parties—such as advertising agencies, Demand Side Platforms (DSPs), Supply Side Platforms (SSPs), and data providers—to process personal data for advertising purposes. These rules are set out primarily by the GDPR and interpreted by the DPA.

When using third-party providers of advertising services, it is not possible to use the ‘customer exception’ under the SSIS as described above, because the third party (agency etc) is not advertising its own similar products or services and is not the entity with which the customer previously entered into a contract. Therefore, such third party must always obtain consent before engaging in direct marketing (emails etc).

In the Czech Republic, failure to have a proper data processing agreement could result in enforcement actions and fines by the DPA—for example Avast Software . was fined CZK 351 million (approximately €14 million) for an unlawful processing of personal data of users of its Avast antivirus program.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter.

In addition see question 5.3 above.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

In addition to EU regulation, there is also national legislation stipulating certain provisions on the use of tracking technologies. The ECA states that entrepreneurs operating public communication networks or providing publicly available electronic communication services are obliged, technically and

organizationally, to ensure the confidentiality of messages and related operational and location data transmitted via their public communication network and publicly available electronic communication services. However, this does not prevent storage of data necessary for the transmission of messages.

The ECA also stipulates that anyone who intends to use or uses electronic communications networks for storage of data or to gain access to data stored in the device is obliged to obtain demonstrable consent from users to the scope and purpose of processing (ie, cookies). The only exception to this is the case of technical cookies (ie, cookies necessary for ensuring the operation of websites and internet services, where obtaining the user's consent is not necessary).

An entrepreneur operating a public communication network or providing a publicly available electronic communication service is also, upon the participant's request, obliged to provide operational and location data available to them based on the ECA, free of charge and in a form allowing further electronic processing of such data, if the participant is not able to record or store such data due to failure on their device resulting from a cyber security incident.

The DPA has issued a recommendation on cookies in the form of FAQs, including ones on:

- (a) pre-set consent in the web browser's setting (does not meet the requirements),
- (b) consent withdrawals (withdrawal of consent must be as easy as the granting of it),
- (c) 'reject all' buttons (should not be significantly smaller or duller than 'accept all', otherwise the consent may not be deemed freely given),
- (d) closing the cookie bar as a form of consent (not permissible).

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

In addition, the DPA has issued guidelines on the obligation of controllers to perform data protection impact assessments ('DPIA'), with a list of activities that are not subject to DPIAs, which list includes loyalty programs and promotions.

In the Czech Republic, loyalty apps are a very common advertising practice which is closely related to privacy regulation. Whilst it is necessary to comply with privacy law, especially minimalization of data accessible to the app and processed by the app, this is not always done. Such apps collect data on purchase history, which is then often used for profiling and targeting advertisement and in some cases transferred to third parties. In its 2025 plan, the DPA is set to inspect the area of data processing through loyalty apps, especially whether personal data are obtained legally and used with consent that complies with GDPR requirements.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

In the Czech Republic, there are no specific regulations concerning social networks and influencer marketing from the perspective of privacy law. Influencer marketing, which is becoming an increasingly important part of product marketing, is addressed primarily from a tax perspective. There is also a specialized self-regulatory initiative for influencer marketing (see question 1.3).

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter and question 7.2.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter.

In the Czech Republic, the age of digital consent under the APDP is set at 15 years. This means that if a child is under 15, companies must obtain verifiable parental consent before processing the child's personal data for purposes such as targeted advertising, account creation, or behavioral tracking. On the other hand, if a child is 15 or older, they can give consent themselves, but companies must still provide information in a child-friendly, clear, and understandable way.

The GDPR also grants children the full suite of data subject rights, including the right to access, rectify, delete, and object to the use of their data, including in advertising contexts. These rights must be actively supported and easy to exercise, with simplified mechanisms that do not burden the user or require excessive effort.

The recently adopted EU Digital Services Act prohibits providers of online platforms from presenting targeted advertising based on profiling using personal data to minors altogether, regardless of consent.

The Advertising Code prohibits manipulative advertising that pressures children to buy products or to persuade their parents to do so. It also restricts the depiction of unsafe behavior, materialism, or misleading health or social claims in child-directed advertising. Meanwhile, the Audiovisual Media Services Directive, implemented in Czech law, restricts commercial content aimed at children on streaming platforms and video-sharing services, with rules including ones against promoting harmful foods, alcohol, or unrealistic beauty standards.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

In addition to the GDPR, AI and its use is regulated under the EU AI Act, adopted in 2024. The AI Act targets the use of AI in all areas and introduces obligations for providers and users depending on the level of risk of the AI system, as well as transparency requirements (especially AI generated content). The AI Act will be fully applicable in 2026, with certain exceptions.

The EDPB recently published two educational materials, 'Law & Compliance in AI Security & Data Protection' and 'Fundamentals of Secure AI Systems with Personal Data', which can be used for guidance.

7.11 Are there other specific advertising practices that you wish to discuss?

New advertising practices are becoming increasingly complex, often leveraging advanced technologies like AI, cross-device tracking, and predictive analytics. In the context of privacy and data protection law, many of these new methods are under regulatory scrutiny because they involve the processing of personal data in novel and sometimes intrusive ways.

Specifically, AI driven advertising practices are becoming very popular, as they automatically evaluate user's data and can provide the user with targeted advertisement anytime and anywhere. With the spread of smart homes and smart speakers; passive listening, voice data collection, and biometric profiling can become a big problem in the future. Voice data could be considered biometric data, which can qualify as sensitive under GDPR, therefore requiring clear user consent as well as transparency and a broad amount of information provided to users.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter. There are no specific jurisdictions prohibited, so long as the GDPR is complied with.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in the Czech Republic? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

The APDP stipulates specific standards and rules for securing data which apply to personal data processing for the purpose of ensuring the defense and security interests of the Czech Republic.

If a company is not entirely sure whether the level of adopted measures for data protection is sufficient, it can consult the DPA, which can provide guidance in this matter.

Further standards for cyber security are stipulated in the Act on Cyber Security, which is being amended in line with the NIS2 Directive to include a wider range of entities on which obligations are imposed depending on size and sector of activity/business, such as registration with the relevant authority, adopting security measures, providing information on security incidents, supply chain security etc.

There are also specific recommendations for individual areas of business, where self-regulatory bodies in particular prepare methodologies for personal data security in the sector concerned.

9.2 How are personal data breaches regulated in the Czech Republic? What are the requirements for notification and response?

See the European Union chapter.

The DPA usually proceeds in line with the guidelines of the EDPB.

Further, the DPA has issued a short guideline on how to proceed in cases of data security breaches, such as the hacking of a computer on which personal data are processed or stored, leading to a leak of the personal data, their alteration or other misuse; or the loss of paper documents containing personal data.

There is no need to report data breaches in cases where the breach is not likely to result in a risk to the rights and freedoms of natural persons. However, if this is not the case, the controller must report the breach to the DPA within 72 hours, either in writing or in electronic form. Any late notifications must contain due reasons in explanation of the default. The DPA has prepared a form for notification of breach, so that the notifying controller may report the facts of the breach as accurately as possible. The processor has reporting obligation to the controller of personal data.

After reporting the breach, the controller must notify the persons whose personal data has been affected by the security breach if there is a high risk that it will affect their personal rights.

There are the following exemptions from this obligation to notify data subjects:

- (a) the controller had introduced appropriate technical and organizational measures and such measures were used for the personal data affected by the data breach, especially if the measures make the data incomprehensible to anyone who is not entitled to access them (eg, encryption);
- (b) after the security breach, the controller has introduced measures which will eliminate the risk for the affected persons; or
- (c) it would require excessive efforts to fulfil the obligation; in such cases, a public announcement or other effective method shall be used.

In cases where the controller is also regulated under the Act on Cyber Security, it may also be required to report security incidents to the National Cyber and Information Security Agency or other relevant authorities.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

The APDP further stipulates a specific fine of up to €400,000 for breaching the ban on processing of personal data imposed by specific Czech legal regulation.

The fines imposed by the DPA usually do not exceed CZK 500,000 (approx €20,000) and often are significantly lower, but recently, there have been some cases of fines around €200,000–300,000 as well as the highest fine of €14 million.

The SSIS stipulates a fine up to CZK 10 million (approx €400,000) for mass or repeated dissemination of commercial communications by electronic means if not compliant with rules set out in the SSIS.

Fines under the ECA can be imposed up to CZK 50 million (approx €2 million) or up to 10% of the net turnover of the offender for the last completed accounting period, whichever is higher for violating the rules set out for collecting personal data in connection with further use of such data for advertising purposes (especially telemarketing etc).

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

The Czech Republic recently adopted a law on class actions, making class action based on an opt-in principle permissible in consumer protection cases, if the conditions are met.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The DPA has demonstrated active enforcement in privacy-related matters, particularly concerning advertising practices. However, there are not many cases of enforcement and fines are not nearly as high as in other EU countries.

Examples of enforcement:

- (a) **Unsolicited commercial communications:** In November 2023, the DPA imposed a fine of CZK 7,700,000 (approx €310,000) on a transportation company for repeatedly sending unsolicited marketing emails advertising third party products to more than 40 million recipients. Advertisements were included in e-mail messages containing confirmation of purchase, and recipients had no way of refusing these commercial communications in any way. Other legal requirements were also not met, such as clearly and unambiguously labelling such messages or providing clear identification of the entity on whose behalf the commercial communications were being sent.
- (b) **Cookie consent violations:** In 2023, the DPA issued fines totalling CZK 4,443,000 (approx €180,000) on various website operators for breaches related to cookie consent. Violations included uploading cookies without user consent, insufficient information provided to users, and deceptive design patterns influencing consent choices.
- (c) **Data misuse by Avast:** In 2024, the DPA imposed a fine of CZK 351 million (approximately €14 million) on Avast Software for transmitting pseudonymized internet browsing data of around 100 million users to its subsidiary, Jumpshot, Inc. The data was shared with marketers for consumer tracking without proper anonymization or legal basis.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in the Czech Republic?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

A hot topic currently under revision by the DPA is the use of 'consent or pay' models by major Czech online news platforms. The choice presented to users is either view content with advertisements (including targeted advertisement and use of cookies—with non-targeted advertisement as an alternative paid option) or pay for viewing the same content. This has led to a number of complaints

by the public. The DPA has started proceedings, considering whether such consent is compliant with the GDPR and whether protection of personal data is being treated as a commodity rather than a basic right. The ongoing proceedings may lead to major fines imposed on some of the biggest local websites and to clarification of admissible practices in data gathering for advertisement purposes.

Regarding legal challenges, in the near future, there will be a considerable amount of new national legislation, implementing EU Acts, such as Digital Services Act, Data Act, Data Governance Act, Digital Markets Act and the Artificial Intelligence Act. It is not anticipated that there will be vast differences from the rules set out in the EU legislation, however Czech law often tends to be stricter in some areas.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The DPA often issues guidelines, recommendations and FAQs concerning specific issues of data protection, and also encourages companies to consult with it. It is advisable to abide by those guidelines and recommendations.

It is also highly advisable to cooperate with the DPA and to be transparent to data subjects in cases of security breaches or misconduct, as the DPA responds well to efforts to remedy such situations.

The DPA, which generally used to impose lower fines, has shifted its decision-making practice slightly and a recent tendency to impose higher fines can be seen.

We also see the common practice in disputes (most often in employment relationships) for one party, in order to put pressure on the other party, or to cause them administrative difficulties and increase their workload, to request complex information and copies of their personal information, or to file complaints with the DPA.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There continues to be constant media coverage of GDPR-related fines as well as possible and emerging regulation of new technologies, especially AI. This contributes to a relatively high level of awareness of data subjects' rights, both on the side of companies and subjects.

Possibly the most obvious change was triggered by the change of cookies regulation (ePrivacy Directive and subsequently change of the ECA), forcing all cookie banners to be changed to opt-in rather than opt-out. Despite the legislation being in force since 2022, real change and compliance has been delayed and seen mostly in the last two years.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenges companies face is keeping track of evolving technologies and regulations and taking appropriate action to update documentation and internal policies to ensure continuous compliance. This is particularly relevant in view of the upcoming entry into force of the Cyber Security Act.

We expect a tightening of the DPA's approach, given the fundamental differences in the way controls are conducted and fines imposed in different parts of the European Union, which could result in forcing companies to ensure proper compliance in all procedures and internal practices.

12.3 What do you envision the privacy landscape will look like in five years?

In the area of personal data and advertising, we expect further development of personalized advertising content, while also anticipating that this development may be based on AI systems linked to everyday applications and consumer activities. We also expect stricter regulation of AI-linked systems, including in the areas of advertising and personal data.

We also expect increased regulation of advertising content on social networks and on the internet in general, especially with regard to children and disadvantaged groups.

We anticipate that all online and internet information and streaming services related to the consent or pay process will continue to be addressed, which may generally mean that some groups of people will only receive limited advertising.

In the Czech Republic, advertising for gambling and alcohol, which is currently only slightly restricted, could be further limited.

 DENMARK 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Denmark.

Privacy is regulated by both applicable Danish law and European law. The primary regulatory legislation is the General Data Protection Regulation ('GDPR') of the European Union. The GDPR is directly applicable in Denmark. Apart from the GDPR, Denmark also has an Act on Data Protection ('Data Protection Act'). This Act supplements the GDPR and implements the elements thereof that are left up to the individual member states of the European Union.

Both the GDPR and the Data Protection Act are interpreted and enforced by the Danish Data Protection Authority ('DDPA') and by the courts. The DDPA has issued and continues to issue its own guidelines for the applicable privacy law in Denmark, in particular relating to the regulation of the GDPR. The guidelines are merely the DDPA's interpretation of the law. They are meant as guidance and are thus non-binding; however, since the DDPA is the overseeing data protection authority that decides whether to report data protection breaches to the police, and since the DDPA has an active role in such a police investigation, one should adhere to the DDPA's guidelines.

1.2 What are the primary laws regulating privacy in Denmark? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The GDPR and the Danish Data Protection Act are the two key pieces of legislation regulating privacy in Denmark. As the GDPR is an EU Regulation, it is directly applicable in all member states, including Denmark.

For the GDPR, please see the European Union chapter.

The Data Protection Act supplements the GDPR and regulates areas in which the GDPR lets each Member State specify their own regulation. Some examples are that the Data Protection Act:

- (a) regulates when a Danish citizen's social security number may be processed;
- (b) specifies when personal data in relation to employment may be used; and
- (c) specifies that personal data may not be transferred for the use of direct marketing, unless the data subject has given their explicit consent.

The use of personal data for marketing is thus regulated in both the GDPR and the Data Protection Act. The Danish Marketing Act, which is the general regulation of all marketing in Denmark, is also relevant, as it regulates when advertisers can use personal information to carry out direct marketing.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Please see the European Union chapter for EU-wide self-regulation programs.

In Denmark, there are no national self-regulatory bodies related to privacy protection, at least not yet.

1.4 How is privacy law enforced in Denmark? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The DDPA is the independent authority in Denmark that supervises compliance with the rules on data protection in Denmark. The DDPA provides guidance, deals with complaints and makes inspections. Although the DDPA is an independent authority, organizationally, it is placed under the Danish Justice Department.

If the DDPA finds it fitting, it may report breaches of the data protection regulation to the police, which will then start an investigation. Although it is the police and not the DDPA that issues fines, the DDPA will have an active role in the police investigation. The DDPA will also make recommendations as to the size of the fine when it reports the breach to the police.

If the entity that has received the fine wishes to dispute the fine, they may fight it in the courts. Alternatively, if an issued fine is not paid or if the acts for which the fine was issued are not acknowledged as infringements by the alleged infringer, the public prosecutor has the authority to sue the entity for alleged breach of the data protection laws.

Apart from actions that involve the DDPA/public prosecutor, any individual (data subject) who has suffered material or non-material damage as a result of an infringement of data protection laws has standing to file a civil lawsuit against that infringing entity. Pursuant to Danish tort law, however, damages are only awarded if the person claiming to have suffered damages can substantiate an economic loss. It is thus unclear whether a person whose data has not been treated in accordance with the laws on data protection can obtain damages if no economic loss can be substantiated (see question 10.2).

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Denmark?

Please see the European Union chapter.

2.2 Does privacy law in Denmark apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Danish Data Protection Act applies to the processing of data related to data subjects located in Denmark, even if the controller or processor is established outside of the European Union if the data processing concerns:

- (a) the offering of goods or services to data subjects located in Denmark, regardless of whether payment from the data subject is required, or
- (b) the monitoring of data subjects' behavior if such behavior takes place in Denmark.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Denmark?

Denmark directly relies on the GDPR; please see the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Denmark directly relies on the GDPR; please see the European Union chapter.

According to the Danish Data Protection Act, processing of personal data is permitted if the processing is necessary:

- (a) to respect the data controller's or data subject's obligations or rights under labor law;
- (b) for preventive disease control, medical diagnosis, nursing or patient care, or management of medical and health services, and the processing of the information is carried out by a person in the health sector who is subject to confidentiality by law;
- (c) for reasons of public interest in the public health field, eg, protection against serious cross-border health risks, or ensuring high quality and safety standards for health care and medicines or medical devices on the basis of EU or national law, which provide for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular confidentiality; or
- (d) for archival purposes in the interest of the public, for scientific or historical research purposes, or for statistical purposes, and is proportionate to the objective pursued, respects the essential content of the right to data protection, and ensures appropriate and specific measures to protect the fundamental rights and interests of the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Denmark directly relies on the GDPR; please see the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Yes. Denmark directly relies on the GDPR; please see the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. Denmark directly relies on the GDPR; please see the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes. Denmark directly relies on the GDPR; please see the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Denmark directly relies on the GDPR; please see the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Denmark directly relies on the GDPR; please see the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Denmark directly relies on the GDPR; please see the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Denmark directly relies on the GDPR; please see the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Denmark directly relies on the GDPR; please see the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Denmark directly relies on the GDPR; please see the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Please see the European Union chapter.

Direct marketing, including emails, texts, push notifications and the like, is specifically regulated in the Danish Data Protection Act and the Danish Marketing Act.

The Data Protection Act dictates that a company may not transfer information about a consumer to another company for the purpose of direct marketing, or use the information for the purpose of direct marketing, unless the consumer has given its specific, express consent.

Moreover, the Marketing Act requires a specific, express consent for sending direct marketing to consumers. It also requires that it is easy and cost-free for the consumer to withdraw consent. Companies may send direct marketing to an email address that they have received from a consumer in connection with a sale, even without consent. Such marketing emails may only concern products or services related to the sale for which the email was obtained. However, companies must make it easy, clear and without cost to decline such direct marketing.

The requirements for consent are the same as in the GDPR. The consent can be given both for data processing and for receiving direct marketing at the same time.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Denmark relies on EU law to regulate this issue; please see the European Union chapter regarding, in particular, the GDPR and the ePrivacy Directive.

7.3 How are loyalty programs and promotions regulated under privacy law?

Denmark relies on EU law to regulate this issue; please see the European Union chapter regarding, in particular, the GDPR and the ePrivacy Directive.

7.4 How is social media and influencer marketing regulated under privacy law?

Insofar as this question relates to data and privacy law, Denmark relies on the GDPR; please see the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Denmark relies on EU law to regulate this issue; please see the European Union chapter regarding, in particular, the GDPR and the ePrivacy Directive.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Denmark relies on EU law to regulate this issue; please see the European Union chapter regarding, in particular, the GDPR and the ePrivacy Directive.

7.7 How is location-based advertising regulated under privacy law?

Denmark relies on EU law to regulate this issue; please see the European Union chapter regarding, in particular, the GDPR and the ePrivacy Directive.

7.8 How are data brokers defined and regulated under privacy law?

To the extent that the activity of data brokers relates to data and privacy law, the question is regulated by the GDPR; please see the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

To the extent that advertising aimed at children is a question of privacy law, the question is regulated by the GDPR; please see the European Union chapter.

Please note that Denmark has decided that ‘children’ in this context are persons under the age of 15.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

As regards profiling and automated decision-making only in the context of advertising, the question is regulated by the GDPR; please see the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

None that relate to privacy specifically. It should, however, be borne in mind that, as alluded to in the above answers, central elements and restrictions related to advertising and marketing under Danish law having nothing to do with privacy and thus fall outside the purview of the present book.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There are strict rules on transferring data across jurisdictions. The question is regulated by the GDPR; please see the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Please see the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Denmark? Are there minimum standards? Does this differ by sector or size of the entity?

Data breaches are addressed by the DDPA. Breaches may be reported to the DDPA on their website, <https://www.datatilsynet.dk/>.

The legal framework used by the DDPA is the GDPR; please see the European Union chapter.

9.2 How are personal data breaches regulated in Denmark? What are the requirements for notification and response?

Please see the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Violations of the GDPR and the Danish Data Protection Act can lead to fines or imprisonment of up to six months. These penalties apply to breaches of core principles such as lawful processing, consent, data subject rights, and data transfers.

Legal persons, including companies and, in some cases, public authorities, may also be held criminally liable.

The DDPA has the authority to issue administrative fines and, in less serious cases, may offer a fine notice as an alternative to prosecution.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers in Denmark have a private right of action under both the GDPR and national law. Data subjects or their representatives may lodge complaints with the DDPA concerning the unlawful processing of personal data. If the DDPA fails to act or the response is unsatisfactory, the matter can be brought before the courts.

Individuals who have suffered either material or non-material damage due to a data protection breach also have the right to seek compensation through legal proceedings. This right is grounded in Article 82 of the GDPR, which provides for judicial remedies in the event of data protection violations.

Entities fined for breaches of data protection law may contest the penalty in court. If a fine remains unpaid or the alleged violation is disputed, the public prosecutor may initiate legal proceedings against the infringing party.

In addition to enforcement by the DDPA or public prosecutor, individuals may pursue civil claims for compensation. Under Danish tort law, compensation requires proof of economic loss, creating uncertainty about whether purely non-economic harm—which one must expect to be the most common harm caused by data breaches—qualifies for damages. Nevertheless, there is growing legal support for compensating non-material damage under Article 82, which states ‘Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered’.

Recent case law, including preliminary rulings from the CJEU, supports the view that Article 82 encompasses non-economic harm—see the words ‘non-material damage’. In particular, the CJEU’s judgment in Case C-590/22 reinforces this interpretation. The Danish Eastern High Court has aligned with this position, referencing CJEU rulings in a case involving claims for non-material, non-economic damage. While the court ultimately found insufficient evidence of unauthorized access to data in that case, it seemingly acknowledged the legal basis for such claims.

Furthermore, limiting compensation under the GDPR solely to economic losses would risk undermining the Regulation’s objective of providing effective redress and robust protection for individuals. Excluding non-economic damages would weaken the deterrent effect of civil remedies and be contrary to the comprehensive enforcement framework of the GDPR.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Since 2019 the DDPA has published on its website an average of just over 60 decisions per year. Few of these decisions have related to advertising or gave rise to court cases. Of those that did, examples include:

- (a) The DDPA assessed that the benefits of membership in a shopping center’s customer club, Goodie, in exchange for consent to marketing, fell within the framework of an incentive that a data controller may offer to obtain consent, without such consent being considered to be in violation of the requirement for voluntariness as understood in the GDPR;
- (b) The DDPA found that there were grounds to issue criticism regarding a telecoms company’s disclosure of the complainant’s email address to Meta Ireland for marketing purposes, as this was not carried out in accordance with the GDPR;
- (c) The DDPA issued a decision regarding the use of a cookie wall on the website of a digital newspaper. The Agency found that the newspaper’s approach—where users could only access embedded content on the newspaper’s website by consenting to the processing of personal data for statistical and marketing purposes—did not meet the requirements for valid consent under the GDPR. The reason was that users were not genuinely presented with a free choice, as the newspaper did not offer an alternative way to access the content alongside the consent request. Consequently, the Agency found grounds to issue an order requiring the newspaper to ensure that the consent obtained from users on its website complies with the requirements of the GDPR.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Denmark?

None.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

As with most areas of law, AI is a hot topic. It is, in part, regulated in the GDPR and the AI Act of the EU. AI is, however, a fast-evolving field, and it is hard to imagine that it will not give rise to legal challenges (or at least growing pains) in the coming years. A direct example of how AI may impact the GDPR system is that DDPA will be the Danish overseeing body pursuant to the AI regulation.

Another critical issue is international data transfers, particularly to countries outside the European Union, particularly the United States. The European Union and the United States have made several attempts to establish compliant frameworks, most recently with the adoption of the EU-US Data Privacy Framework on 10 July 2023. However, previous arrangements were invalidated by the CJEU, and the new framework is already facing scrutiny. A legal challenge has been filed by French MP Philippe Latombe (Case T-553/23) seeking to annul the Commission’s adequacy decision.

There is still some debate as to whether ‘non-material damages’ in Article 82 of the GDPR must be interpreted as requiring Member States—in spite of their national legal traditions—to award damages for non-economic harm.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The issue of whether personal data may be used as ‘payment’: For example, the Danish Sale of Goods Act defines the supply of digital content or a digital service when the supply is provided in exchange for personal data, unless the data is processed solely for the purpose of supplying the digital content or digital service, or to enable compliance with legal obligations as a ‘consumer purchase’.

This would seem to mean that providers of digital services such as social media cannot rely on consent for their data processing, as the GDPR states that: ‘When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.’ In such cases, there is a presumption that consent is not freely given, meaning that there is a presumption that the consent is not valid.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The implementation of the EU-US Data Privacy Framework in 2023. It shall be interesting to see if it lasts.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Generally, transfers to third countries can pose a challenge. Most companies are not aware of just how restricted the options are for transferring data to third countries.

This has led the Commission to consider simplifying various requirements under the GDPR to lessen the administrative burden on companies in the European Union and heighten the competitiveness on the international market of EU-based companies.

12.3 What do you envision the privacy landscape will look like in five years?

Notwithstanding unforeseen technological advances, including the field of AI, the present author imagines that the slow and steady progress will simply continue.

 FINLAND 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Finland.

There is a constitutional right to privacy under Finnish law. By the Constitution of Finland (731/1999, as amended) everyone's private life, honor and the sanctity of the home are guaranteed, and the secrecy of correspondence, telephony and other confidential communications is inviolable (the 'right to privacy'). Public authorities and businesses exercising public functions are obliged to comply with the requirements of the European Convention on Human Rights, which include a general right to privacy.

Finland is an EU Member State and consequently the EU General Data Protection Regulation (2016/679) ('GDPR') is directly applicable in Finland (see the European Union chapter). Finland's Data Protection Act (1050/2018) ('DPA'), which supplements the GDPR, became applicable on January 1, 2019. (The main national additions or specifications to the requirements of the GDPR are set out in question 1.2.)

In addition to the general data protection laws, there are also several sector-specific data protection and privacy laws. For example, the processing of employee data and privacy of electronic communications are quite heavily regulated in Finland (see question 1.2).

1.2 What are the primary laws regulating privacy in Finland? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

In addition to the GDPR:

- (a) The DPA supplements and provides more specifics on certain parts of the GDPR. The main national additions or specifications to the requirements of the GDPR include the following:
 - (i) **Age limit for consent when offering information society services to children:** The national age limit for when consent can be given by a child in relation to information society services has been set to 13 years. Thus, for processing personal data of children under this age, parental consent is required;
 - (ii) **Specifications regarding administrative fines:** Administrative fines may not be imposed on public authorities or bodies in Finland;
 - (iii) **Sanctions:** In addition to administrative fines or other sanctions, criminal sanctions are included in the Criminal Code of Finland (39/1889), and a new criminal offence, 'data protection offence', applicable only to natural persons, has been introduced;
 - (iv) **Provisions on national discretion:** The DPA includes national regulation on processing of specific types of data, such as health-related data, personal identification numbers, and children's personal data; and
 - (v) **Supervisory authority:** The competent local supervisory authority continues to be the Finnish Data Protection Ombudsman. (The Finnish Transport and Communications Agency ('Traficom') remains the supervisory authority in e-privacy matters.)
- (b) Finland's data protection laws also include separate provisions on the processing of employees' personal data, which are set out in the Act on the Protection of Privacy in Working Life (759/2004). This Act applies to the relationship between employers and employees, and

includes restrictions on, for example, the processing of employee health data and credit data, conditions for carrying out drug tests and camera surveillance, as well as regulation on personality assessments and the retrieval and opening of employees' electronic messages.

- (c) Further, information society services are governed by the Act on Electronic Communications Services (917/2014) which, inter alia, implements the ePrivacy Directive. In addition to, for example, provisions relating to the use of cookies (see, further, question 7.2), this Act contains strict rules on the confidentiality of electronic communications and electronic monitoring. Privacy of communications covers both the content of communications (such as content of emails) as well as traffic data (ie, such metadata of communications that is used for transmission thereof and that can be associated with a legal or natural person). Confidentiality of electronic communications is media neutral (and thus covers also over-the-top services, eg, chat functions in apps and on webpages). See, further, question 7.1.
- (d) The Criminal Code of Finland contains several criminal sanctions relating to privacy matters, such as the data protection offence.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

See the European Union chapter.

1.4 How is privacy law enforced in Finland? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

In Finland, the Data Protection Ombudsman (tietosuojavaltuutettu) is the local supervisory authority which supervises compliance with general data protection legislation. The Data Protection Ombudsman is responsible for supervising compliance with data protection legislation and other laws concerning the processing of personal data, carrying out investigations and inspections, and imposing administrative sanctions for violations of the GDPR.

Traficom is the supervisory authority in e-privacy matters.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Finland?

See the European Union chapter.

In addition, pursuant to the DPA, the processing of personal data is governed by Finnish laws if the controller's place of business is located in Finland, and if the processing is carried out in the context of the activities of an establishment of a controller or processor in the European Union.

2.2 Does privacy law in Finland apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, Finnish privacy law applies to foreign companies. With respect to the GDPR, please refer to the European Union chapter.

Neither the Act on Protection of Privacy in Working Life nor the Act on Electronic Communications Services contains clear provisions specifying their territorial reach. However, in the employment context, the provisions of these Acts should generally be limited to employees who work for a local office in Finland or where the employment contract is governed by Finnish law.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Finland?

Personal data is legally defined in the GDPR (see the European Union chapter). No separate definition is contained in the DPA.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

In addition, the DPA provide exceptions where the general prohibition on processing special categories of personal data in the GDPR is not applied. Listed below are examples of particularly relevant cases where special categories of data may be processed:

- (a) special categories of personal data may be processed by insurance companies for the purpose of clarifying their liabilities;
- (b) any processing of data that is provided by law or that derives directly from a statutory duty set out for the controller by law;
- (c) special categories of personal data may be processed for the purposes of scientific or historical research and statistical purposes; and
- (d) personal data related to criminal convictions and offences for the purposes of legal proceedings.

According to the DPA, when processing special categories of data, the controller and the processor must take appropriate and specific steps to ensure the protection of the rights of the data subject. Some of these steps are specified in the DPA, such as pseudonymization, encryption and appointing a data protection officer.

Consent to the processing of sensitive personal data must be explicit. Note that the age at which a child can provide a valid consent in relation to information society services has been set at 13 years, whereas the default option in the GDPR is 16 years (see question 1.2).

In addition, the Act on the Protection of Privacy in Working Life sets extensive restrictions on the processing of personal data in the context of employment relationships. Personal data should primarily be collected from the employees themselves, and from third parties only with the employee's consent. Unnecessary personal data of employees cannot be processed even with the employee's consent.

Finally, the DPA contains restrictions on the processing of personal identification numbers.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, see the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, see the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for privacy law obligations.

The requirements for direct electronic marketing are set out in the Act on Electronic Communications Services, which provides the following rules for marketing communications for private individuals:

- (a) Direct marketing by means of automated calling systems, fax, or email, text, voice, sound or image messages requires prior consent by the consumer (opt-in).
- (b) Other direct marketing (such as phone marketing or letters) is allowed if the individual has not specifically prohibited it (opt-out). The consumer must be able easily, and at no charge, to prohibit direct marketing.
- (c) Where a service provider has obtained a customer's contact information relating to email, text, voice, sound or image messages in the context of the sale of a product or a service, such service provider may use this contact information for direct marketing of their own products of the same product group and of other similar products or services. The customer must be given the opportunity to prohibit, easily and at no charge, the use of such contact information at the time when it is collected and in connection with any email, text, voice, sound or image message. The customer must be clearly notified of the possibility of such a prohibition (soft opt-in).

In the B2B context, the opt-out model applies, assuming that the content of the marketing message is relevant for the recipient of the marketing message considering the recipient's position in the organization.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

Cookies are regulated in national legislation under the Act on Electronic Communications Services. Under this Act, a service provider may save cookies or other data concerning use of the service in the user's terminal device, and use such data, if the user has given consent to this and the service provider has given the user comprehensible and complete information on the purposes for which such data is to be saved or used. Note that these provisos do not apply to any storage or use of data which is intended solely for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

Traficom, which is the competent national authority, updated its guidelines on cookies in late 2021 to reflect the CJEU ruling in the Planet49 case, and accordingly any opt-out consent by way of pre-ticked checkbox is insufficient for the storage of cookies.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

- 7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

See the European Union chapter, and questions 7.1 and 7.2 above.

- 7.6 How are digital identity resolution and clean room technologies regulated under privacy law?**

See the European Union chapter.

- 7.7 How is location-based advertising regulated under privacy law?**

See the European Union chapter.

- 7.8 How are data brokers defined and regulated under privacy law?**

See the European Union chapter.

- 7.9 How is advertising to children and minors regulated under privacy law?**

See the European Union chapter.

- 7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?**

See the European Union chapter.

- 7.11 Are there other specific advertising practices that you wish to discuss?**

N/A

8 DATA TRANSFERS

- 8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?**

See the European Union chapter.

- 8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?**

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

- 9.1 How is data security regulated in Finland? Are there minimum standards? Does this differ by sector or size of the entity?**

See the European Union chapter.

- 9.2 How are personal data breaches regulated in Finland? What are the requirements for notification and response?**

See the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter and question 1.2 above.

In addition, for those infringements of the GDPR or the DPA that are not subject to administrative fines, the DPA refers to Criminal Code of Finland. Breaches of the GDPR or Finnish data protection legislation may constitute a data protection offence, message interception or violation of a confidentiality obligation, computer break-in, illicit viewing, or eavesdropping. Criminal sanctions range from fines to imprisonment for a maximum term of 1–3 years, depending on the type and level of the offence.

Further, according to the Act on Protection of Privacy in Working Life, if an employer or a representative of the employer breaches an obligation or restrictions regarding processing personal data in the context of employment, the employer will be sentenced to a fine, unless a more severe penalty is provided in another Act.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

See the European Union chapter.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Finland?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

GDPR enforcement (including enforcement trends in the European Union) and continuously developing case law is something to monitor. Furthermore, the increased use of AI tools poses privacy concerns.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

See the European Union chapter.

12.3 What do you envision the privacy landscape will look like in five years?

The privacy landscape is expected to look fairly similar in five years, although the EU Commission is currently considering possible amendments to the GDPR framework.

FRANCE

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in France.

Privacy is regulated by statutory law and European Law. These Laws are interpreted and enforced by the supervisory authority ('CNIL'), which is a governmental authority, but also by French courts. CNIL acts in the following four main fields of activity:

- (a) to inform individuals of their rights and data controllers/processors of their obligations (and accompany them in their compliance process),
- (b) to issue its own guidelines interpreting the law,
- (c) to sanction the violation of its guidelines (investigatory powers, warnings, cease and desist letters and sanctions, including monetary sanctions), and
- (d) to issue public communications (opinions at the request of the legislator, or public communications pertaining to innovation/prospective).

CNIL's guidelines and opinions are not binding on the courts but are usually considered by the judges.

Privacy has been regulated in France since the law dated January 6, 1978 ('Data Protection Law'). It was amended in 2018 to introduce the necessary changes (ie, opening clauses) required by the European General Data Protection Regulation ('GDPR').

As the most important aspects of data privacy are regulated by the GDPR, France has only very limited regulatory power. The rules which are not subject to national regulation, or for which France has not made use of an opening clause, will only be mentioned below by a short reference on the European Union.

1.2 What are the primary laws regulating privacy in France? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary source for data protection in the European Union, and thus in France, is the GDPR, which is directly applicable in all European Member States and does not need to be implemented by the individual European Union Member States. The GDPR covers most of the privacy regulation.

The Data Protection Law aims at implementing the opening clauses; the main rules aimed at completing the GDPR are the following:

- (a) the implementation of the accountability principle led to the withdrawal, from French law, of the obligation to file a data processing activity with the CNIL (which was compulsory before the GDPR entered into force), except for specific data processing, for the collection/processing of French citizen's social security identification number (ie, this still requires the authorization of the CNIL);
- (b) sensitive data cannot be processed except in limited instances provided by law (eg, when the processing relates to data which has been anonymized, or when the processing concerns public information mentioned in court decisions, provided that the purpose and the consequences of the processing do not lead to the re-identification of the individual concerned);
- (c) the processing of health data must be authorized by CNIL in certain instances, in particular, processing for research purposes when the processing does not meet the guidelines issued by CNIL;

- (d) children must be at least 15 years old to give a valid consent for the processing of their personal data (the GDPR sets the age at 16 years, but EU Members States are allowed to provide for a lower age); to protect children from social networking sites, the law of July 7, 2023 laid down a digital age of 15 for registering on these sites (platforms will have to implement a technical solution);
- (e) when the processing is based on the consent of the data subject, the controller must be able to demonstrate that the contracts which relate to devices or services leading to the processing of personal data do not prevent consent of the end user. Consent may be deemed prevented when the end user is faced with restrictions, without legitimate technical or security reasons, during the initial configuration of the device; and
- (f) the notification of a data breach to a data subject can be restricted when such a notification could raise an issue relating to national security, defense or public security.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

France does not have any self-regulatory body which can enforce privacy law. CNIL issues guidelines and opinions though (see question 1.1).

1.4 How is privacy law enforced in France? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The GDPR and the Data Protection Law are enforced by CNIL, which has the following powers (see also question 10.3):

- (a) to handle claims filed by individuals;
- (b) to carry out investigations (as a supervisory authority) and to issue corrective measures in the event of a violation of privacy law (eg, warnings, cease and desist letters, withdrawal of an authorization issued by CNIL, prohibition to carry out the processing, imposition of fines etc); and
- (c) to inform the prosecutor of any violation of the privacy law and to submit observations during a criminal procedure.

The French courts also have jurisdiction if a lawsuit is brought by data subjects claiming that their rights have been violated and claiming a civil or criminal liability (depending on the violation) from the data controller or processor.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in France?

See the European Union chapter.

In addition to the scope of the GDPR, the Data Protection Law applies to any processing carried out in connection with the activity of the establishment of a data controller (or its data processor) where this establishment is located in France (irrespective of the place where the processing is located, whether in France or abroad).

2.2 Does privacy law in France apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law applies to foreign companies as follows:

- (a) As far as the GDPR is applicable, it applies to a data controller located outside France.
- (b) The rules in the Data Protection Law enacted to implement the opening clauses of the GDPR apply if the data subject resides in France (irrespective of whether or not the data controller is established in France); there is, however, an exception for processing carried out for journalistic, academic, artistic or literary purposes, whereby the Data Protection Law applies to the data controller when it is established in the EU.

See the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in France?

The Data Protection Law states that it applies to all or part of the automated processing of personal data, as well as to the non-automated processing of personal data contained or intended to be contained in files, with the exception of processing carried out by natural persons for the exercise of strictly personal or domestic activities.

According to the Data Protection Law, a ‘personal data file’ is any structured set of personal data accessible according to specific criteria, whether this set is centralized, decentralized or distributed functionally or geographically.

The Data Protection Law also states that, unless otherwise provided, the definitions in the GDPR apply. Thus, the definition of ‘personal data’ is that set out in the GDPR. See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

In addition to specific obligations contained in the GDPR, the Data Protection Law sets forth exceptions to the prohibition of the processing of sensitive data, eg, if:

- (a) the processing concerns statistics and is carried out by the French national authority in charge of statistics and economic studies, or by a service of a Ministry in charge of statistics (This exception is more restrictive than the corresponding exception set forth by the GDPR); or
- (b) processing concerns public information mentioned in court decisions, provided that the purpose and the consequences of the processing do not lead to the re-identification of the individual concerned (see question 1.2).

The controller or processor must take appropriate and specific measures to safeguard the interests of the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

As anonymization and de-identification techniques are bound to evolve regularly, it is essential for any data controller concerned to keep a regular watch to ensure that the anonymous nature of the data

produced is preserved over time. This monitoring must consider the technical means available, as well as other sources of data which may make it possible to remove the anonymity of information.

If a dataset published online as ‘anonymous’ actually contains personal data, and no exception is applicable (the French Public-Government Relations Code provides that in certain circumstances, and provided that certain rules are complied with, the French administration is entitled to publish administrative documents), this may be considered a data breach. It is then necessary to:

- (a) remove the data set in question as quickly as possible;
- (b) inform the CNIL if the breach is likely to pose a risk to the rights and freedoms of individuals; and
- (c) inform the individuals concerned if the risk is high.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter and question 5.3.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter and question 1.4.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

On June 23, 2022, the CNIL sanctioned Total Energies Électricité and Gaz France (a French energy producer and supplier) for violating the Data Protection Law and ordered the company to pay a fine in an amount of €1,000,000.

This company had made available, on its website, a form for the subscription to an energy contract in which subscribers had to agree to the use of their personal data to receive further commercial communications; by filling in this form, users had no means to opt-out of the use of their personal data for direct canvassing purposes for similar products or services, in violation of the French Post and Electronic Communications Code.

The investigations carried out by CNIL also revealed four other breaches of the GDPR:

- (a) **a breach of the obligation to inform individuals canvassed by telephone:** The core information concerning the processing of their personal data was not shared with the individuals during the call; they were also not offered the opportunity to have access to further information, eg, by pressing a key on their telephone keypad.
- (b) **a failure to comply with the data subject's (i) right of access and (ii) right to object to the processing of their personal data at any time:** The company failed to comply with the complainants' requests to access their personal data and to stop receiving direct canvassing phone calls.
- (c) **failure to comply with the obligations pertaining to the way to exercise these rights:** The company failed to answer queries within the one-month period imposed by the GDPR.

CNIL's report, published in 2025 (for activity carried out in 2024), shows that infringements of the GDPR in the context of commercial direct canvassing are recurrent (eg, an email provider inserting advertisements between emails received in users' inboxes without previously obtaining their consent).

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter and question 5.3.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

The Data Protection Law also implements the EU ePrivacy Directive into French law. It lays down the obligation, subject to certain exceptions, to obtain the consent of Internet users prior to any operation involving the writing or reading of cookies and other trackers.

On July 4, 2019, CNIL issued revised Guidelines pertaining to the use of tracking technologies such as cookies, which are now in line with the GDPR concerning the need for the explicit consent of the internet user, as set forth by the GDPR. (The former version of these guidelines was no longer compliant with the GDPR (the fact that an internet user continues browsing was deemed a valid consent)).

These Guidelines have been supplemented by a CNIL Recommendation dated September 17, 2020, to inform operators on practical methods to obtain internet users' consent (see question 7.5).

Finally, on May 16, 2022, CNIL published Guidelines to set out the main principles to be complied with by website editors intending to use cookie walls and pay walls. CNIL recommends, for instance, that, when an Internet user refuses the use of cookies on a website (eg, by clicking on a 'reject all' button), the website's editor offers a real and fair alternative that allows access to the website and does not require consent to the use of personal data. Otherwise, the editor must be able to demonstrate that its service is also accessible on another website without a cookie wall. In such a case, CNIL recommends that the website editor using a cookie wall ensures that the alternative is easily accessible to the Internet user, to avoid any imbalance between the editor and the Internet user, which could deprive the latter of a real choice.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

CNIL considers that, while certain tracking technologies are exempt from the requirement to obtain consent (such as those used for authentication with a service, those used to keep track of the contents of a shopping cart on a merchant site, certain cookies used to generate traffic statistics, or those that allow paying sites to limit free access to a sample of content requested by users), the users must, nonetheless, be informed of the use of these tracking technologies, for instance in the privacy policy governing the use of the website.

Moreover, concerning the tracking technologies the use of which requires the user's consent, CNIL recommends that the interface used to gather the consent not only includes an 'accept all' button but also a 'refuse all' button.

In addition, CNIL recommends that websites, which generally retain consent to trackers for a certain period, should also retain the refusal of users for a certain period of time, so as not to re-ask the user each time they browse on the website.

Finally, to ensure that the user is fully aware of the scope of their consent, CNIL recommends that, when tracking devices are used on websites other than the one visited, consent be obtained from each of the sites concerned by the tracking activity.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

On June 25, 2018, CNIL served formal notice on TEEMO and FIDZUP (ad targeting service providers using geolocation) to comply with the GDPR and the Data Protection Law. It found a breach of the obligation to obtain the consent of the data subjects concerned prior to the processing of their data. Following a study of these collections via SDKs, the CNIL indicated that: (i) TEEMO and FIDZUP were data processors, and (ii) the consent of data subjects has not been collected in a prior, clear, free and specific manner, in accordance with the requirements of the GDPR. The processing operations were therefore unlawful.

Indeed, geolocation data is indirect personal data, since it enables the identification of a person when combined with direct identification data and provides information on their location and movements. Consequently, the collection and use of such data for profiling and targeted marketing or advertising purposes requires data controllers to ensure that they have a legal basis—in this case the individual's prior consent.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter.

On November 28, 2022, CNIL was invited by regulatory authority for audiovisual and digital communication ('ARCOM') to sign a Charter by which online platform operators undertake to promote the reporting of content harmful to minors and prevent the commercial processing of their personal data.

ARCOM regulates content broadcast on various media (eg, TV, radio) to limit the exposure of minors to shocking content that is inappropriate for their age and development.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

In February 2025, CNIL published two new recommendations for AI use that respects personal data, confirming that the requirements of the GDPR are sufficiently balanced to address AI's specificities. These recommendations offer concrete and proportionate solutions to inform and facilitate the exercise of people's rights:

- (a) When personal data is used to train an AI model and is potentially stored by it, data subjects must be informed.
- (b) European regulations provide for rights of access, rectification, opposition and deletion of personal data. However, these rights can be particularly difficult to implement in the context of AI models, whether to identify individuals within the model or to modify the model. CNIL calls on businesses acting in this field to make every effort to take privacy protection into account right from the model design stage. It invites them to pay particular attention to the personal data present in training databases by:
 - (i) striving to make models anonymous, where this is not contrary to the objective pursued; and
 - (ii) developing innovative solutions to prevent the disclosure of confidential personal data by the model.

7.11 Are there other specific advertising practices that you wish to discuss?

CNIL is currently working on a draft recommendation on the use of location data from connected vehicles. This recommendation is intended to make it easier for businesses acting in this field of activity to comply with the most common uses. It focuses on the use of connected vehicles by private individuals, as owners or lessees. The use of company cars made available to employees by their employer, for which CNIL has already issued recommendations, is therefore not covered by this draft.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in France? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

9.2 How are personal data breaches regulated in France? What are the requirements for notification and response?

See the European Union chapter.

CNIL regularly reports on typical data breaches inspired by real-life incidents notified to it.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) **Administrative sanctions:** See the European Union chapter.
- (b) **Criminal penalties:** The French Criminal Code sets forth criminal penalties—eg, the processing (in particular for marketing purposes) of personal data of an individual despite their opposition (or when this opposition is based on legitimate interests) is sanctioned by a prison term of up to 5 years and by a fine of up to €300,000 (when the infringer is an individual) or €1.5 million (when the infringer is a legal entity).

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter and question 1.4 above.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

CNIL is very active in sanctioning GDPR/Data Protection Law violations. In 2024, it issued 180 formal notices and 87 sanctions totaling €55,212,400 (more than doubling in the number of sanctions (42) in 2023). In all, CNIL issued 331 corrective measures.

When breaches of the GDPR or the Data Protection Law are brought to its attention, CNIL's restricted committee is empowered to:

- (a) issue a call to order;
- (b) order the processing operation to be brought into compliance, including under penalty payment;
- (c) temporarily or definitively restrict a processing operation;
- (d) suspend data flows;
- (e) order that requests to exercise people's rights be met, including under penalty payment; and/or
- (f) impose an administrative fine.

Under the GDPR, pecuniary sanctions can be up to €20 million or, in the case of a company, up to 4% of worldwide annual sales. These penalties may be made public.

On June 15, 2023, CNIL fined online advertising specialist CRITEO €40 million for failing to check that the people whose data it processes have given their consent.

On November 14, 2024, CNIL fined ORANGE (internet and communication service provider) €50 million for displaying advertisements between the emails of users of its email service, without their consent.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in France?

The Civil Code provides for a right of privacy, as it states that 'Everyone has the right to respect for his private life. Without prejudice to the indemnification for injury suffered, judges may prescribe any

measures, such as escrow, seizure and others, suited to the prevention or the ending of an infringement of the intimate character of private life; in case of emergency those measures may be provided for by summary proceedings’.

This has been extended/used, by French courts, for the protection of the right of publicity (image, likeness etc), and is also used as a ground of action destined to control the commercial use of someone’s persona.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

The rise of new technologies and digital services (eg, biometrics, artificial intelligence, the Internet of Things, virtual and augmented reality, digital identity etc) has transformed our societies, paving the way for an era dominated by digital technology.

This evolution represents a considerable opportunity for innovation and growth, but requires a delicate balance between data exploitation and respect for privacy. It also raises major ethical concerns.

CNIL has identified three issues at the heart of digital challenges, which warrant particular attention to ensure that innovation remains at the service of citizens.

- (a) The first concerns artificial intelligence and the advent of generative AI, which marks a new digital revolution.
- (b) The second relates to cybersecurity against a backdrop of increasing breaches on a large scale, heightening people’s concerns about the use of their data.
- (c) The third concerns the protection of younger children from the risks associated with overexposure to screens.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

People whose data is collected, used or reused to develop an AI system have rights to their data, enabling them to retain control over it. It is up to data controllers to respect these rights and facilitate their exercise. The exercise of these rights is closely linked to the provision of information on data processing, which is also an obligation.

Data subjects must be able to exercise their rights both:

- (a) on training databases and,
- (b) on AI models if these are not considered anonymous.

While exercising a right of access, rectification or deletion on a training database presents issues comparable to other large databases, exercising these rights on an AI model itself presents particular and unprecedented difficulties. This requires the adoption of realistic and proportionate solutions, guaranteeing the rights of individuals without hindering innovation in artificial intelligence.

CNIL considers that the GDPR makes it possible to address the specific features of AI models for the exercise of rights. The complexity and costs of requests that would prove disproportionate are thus factors that can be considered.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The EU AI Act and other digital regulations were launched as part of the European Digital Single Market (moving from 28 national digital markets to a single one).

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Data privacy laws and regulations continue to change and evolve across the globe, making it difficult for organizations to keep pace with the latest developments. The rise of new technologies and digital services increases the ‘compliance’ challenges for organizations.

12.3 What do you envision the privacy landscape will look like in five years?

CNIL’s European and international strategy 2025–2028 on data protection has three key priorities:

- (a) streamlining European cooperation,
- (b) promoting high international standards of data protection, and
- (c) consolidating its network of influence.

In addition to its strategic plan 2025–2028, CNIL’s European and international strategy aims to strengthen and coordinate its action, in particular by taking into account the orientations of the European Data Protection Board.

 GERMANY 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Germany.

Privacy is regulated by statutory law, such as constitutional rights, federal law, state law and European law. They are all interpreted and enforced by the data protection authorities and, if the addressee of the orders issued by the authorities questions them, by the courts. The data protection authorities issue their own guidelines interpreting the laws. While these guidelines only reflect the opinion of the authorities and are non-binding, they could be used by the courts as a source when assessing the orders issued by the authorities.

Privacy has been a core concern of post-war Germany. The first ever data protection law in the world came into force in 1970 in Germany on a state level. A constitutional ruling from 1983, triggered through a census the same year, even created a new constitutional right: the right for informational self-determination based on Article 2(1) in conjunction with Article 1(1) of the Grundgesetz (German Constitution). It has been described as the ‘very key to the German view on data protection’. The German Federal Constitutional Court ruled: ‘Under the conditions of modern data processing, the protection of individuals against unlimited collection, storage, use and disclosure of their personal data is covered... In this respect, the fundamental right guarantees the right of the individual to determine the disclosure and use of his or her personal data herself or himself.’

This ruling was the basis for the first German Federal Data Protection Act (‘BDSG’) that in large parts was used as a blueprint for the European General Data Protection Regulation (‘GDPR’). The BDSG has to be interpreted in accordance with the principles of the GDPR and may not be used at all where the GDPR provides its own stipulations. The BDSG is now only a secondary, but nonetheless important, source for data privacy protection. It contains not only the sector-specific regulations permitted by the opening clause of the GDPR but also regulations on aspects which are not regulated by the GDPR, such as data privacy in relation to criminal prosecution and proceedings.

All federal states have their own data protection laws (which only regulate processing of data by public bodies).

There are also data protection stipulations in other laws. The most important Act next to the GDPR and BDSG that affects data protection and contains important data protection rules is the German Telecommunications Telemedia Data Protection Act (‘TDDDG’), which was enacted in December 2021. The TDDDG combines all of the data protection regulations of the previous Federal Telecommunications Act and Federal Telemedia Act and, among other things, also regulates the use of cookies on websites in Germany.

As the most important aspects of data privacy are regulated by the GDPR, Germany has only very limited regulatory power. As pointed out earlier, the relevant fields are the sector-specific opening clauses of the GDPR, administrative stipulations and certain aspects of criminal prosecution and enforcement. Those aspects of the GDPR which are not subject to national regulation or for which Germany has not yet made use of an opening clause will only be mentioned below by a short reference to the chapter on the European Union.

1.2 What are the primary laws regulating privacy in Germany? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary source for data protection in the European Union, and thus in Germany, is the GDPR. As a European Regulation, it is directly applicable in all EU Member states and does not need to be implemented by the individual states. The GDPR covers most of the relevant aspects of data privacy.

On the other hand, the GDPR contains several opening clauses, allowing EU Member States to enact national privacy rules on certain aspects, which either specify or limit the rights and obligations contained in the GDPR. Germany has done so, and has included them in the BDSG.

The most important stipulations for the private sector in the BDSG which are based on GDPR opening clauses are the following:

- (a) For certain purposes relating to social security, healthcare and the public interest, private bodies are allowed to process special categories of personal data. The processing of personal data of employees has additional provisions.
- (b) Exceptions to the requirements under the GDPR relating to information to be provided to data subjects apply in certain cases: eg, where confidentiality obligations exist, or if the information would undermine the enforcement of civil claims;
- (c) Further exceptions are made to the data subject's right to cancellation of data;
- (d) More detail is provided as to when a DPO is needed;
- (e) A comprehensive regulation is provided for the protection of employee data.

However, as far as the processing of personal data for marketing purposes is concerned, all relevant stipulations are contained in the GDPR.

While the applicable European, Federal and State laws regulate the processing (use) of personal data, certain aspects of marketing activities, such as direct marketing by email or telephone, are regulated by the German Act against Unfair Competition ('UWG').

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In Germany, self-regulation plays a complementary role in privacy governance, particularly in the advertising sector, but it does not substitute for compliance with statutory requirements under the GDPR, the TDDDG, and the UWG. The following may be noted:

- (a) Sector initiatives, such as the IAB Europe's Transparency and Consent Framework, aim to standardize user consent management. However, German supervisory authorities have raised significant concerns regarding such frameworks' compatibility with GDPR standards, particularly concerning transparency and valid consent. While the GDPR allows for approved codes of conduct, few have been formally recognized in the advertising context.
- (b) Organizations like the German Advertising Standards Council provide ethical guidelines and handle complaints about advertising content. Although such bodies promote responsible advertising, their decisions are not legally binding and do not address underlying data processing activities.
- (c) German consumer associations play an increasingly important part in privacy enforcement. These organizations monitor advertising practices and have brought collective actions against companies for unlawful use of tracking technologies, inadequate privacy notices, or missing consent. Since the introduction of the Consumer Rights Enforcement Act, their role in enforcing privacy rights has gained additional legal standing.

- (d) While self-regulatory efforts may support accountability and internal compliance, they do not replace core obligations, such as obtaining informed consent or providing transparent information. German regulators emphasize that self-imposed standards must not lower the level of protection guaranteed by law.
- (e) Data protection authorities in Germany are open to engaging with industry bodies and consumer organizations when developing practical guidance. However, they remain cautious where self-regulatory mechanisms lack enforceability or where commercial incentives risk undermining data subject rights.

1.4 How is privacy law enforced in Germany? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The GDPR, the BDSG and other laws protecting personal data are enforced by supervisory authorities as well as the competent administrative authority. Supervisory authorities can monitor, ask questions that need to be answered, and issue orders and fines in cases of violations of the data protection laws.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Germany?

See the European Union chapter.

In addition to the scope of the GDPR, the BDSG applies to private bodies if the controller or processor processes personal data in Germany, regardless of whether any establishment of the controller or processor is in Germany or in the European Union, or the data subject being in the European Union.

2.2 Does privacy law in Germany apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law applies outside the country:

- (a) GDPR: as far as the GDPR is applicable, it applies to companies outside Germany;
- (b) BDSG: the BDSG applies to controllers and processors that:
 - (i) process personal data in Germany,
 - (ii) process personal data in the context of the activities of their establishment in Germany, or
 - (iii) do not have an establishment in Germany but fall within the scope of the GDPR.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Germany?

Personal data is legally defined in the GDPR (see the European Union chapter). An identical definition is contained in the BDSG.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

In addition to the specific obligations contained in the GDPR, the BDSG permits private bodies to process special categories of personal data for certain purposes, eg if processing is necessary:

- (a) to exercise the rights derived from the right of social security and social protection and to meet the related obligations; or
- (b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision.

The controller or processor must take appropriate and specific measures to safeguard the interests of the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under German and EU data protection law, the treatment of anonymized, pseudonymized, and de-identified data is primarily governed by the GDPR and interpreted in light of national guidance, particularly by the German data protection authorities. Note that, in enforcement and legal practice in Germany, the threshold for considering data anonymized is high. Controllers must demonstrate that re-identification is not reasonably possible, considering technical capabilities and contextual factors.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies operating in Germany must comply with the GDPR and the BDSG, which impose comprehensive obligations on controllers and processors. Obligations vary, depending on the services provided, as well as the type and volume of data and the size of the company. See the European Union chapter.

Of particular note is that, under German law, a DPO is required where at least 20 employees are regularly involved in automated data processing, or where sensitive data is processed on a large scale.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter for privacy law obligations.

In addition:

- (a) Certain direct marketing activities, such as email, telefaxes, text messages and phone calls are subject to the UWG, and are, as a general rule, only permissible on the basis of a valid prior and informed consent regarding the specific means of direct marketing and the product or services to be marketed. The GDPR requirements for the use of the data (consent or legitimate interests) do not serve as a basis for permission in this respect, as they relate only to the use of the data, not to the specific means of marketing. But the consent may be valid for both if addressed correctly.
- (b) Competitors, consumer protection associations, industry associations and recipients of the marketing communication are able to enforce the law using warning letters and court orders by (preliminary) injunction.
- (c) No pre-checked boxes are allowed. If consent is contained in other clauses (eg, of standard terms), it must be highlighted.
- (d) In the case of online consent, eg, for newsletters or mailings, a two-factor authentication is necessary in order to be able to show evidence of a valid consent by the person identifies by the data relating to the consent. This is usually achieved by the so-called ‘double opt-in’. With the double opt-in procedure, the user first indicates on a website that they would like to receive information by email in the future. In a second step, a confirmation mail containing a confirmation link is sent to the email address provided. The recipient has the option to confirm the consent to receiving future advertising or information mails by clicking on the confirmation link. This is to prevent the misuse and illegal processing of email addresses and helps the sender to document the explicit consent should he later be in need to prove the consent. A German district court has decided it is not in accordance with the law to place advertisements in the confirmation mail itself.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See question 5.1.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

In Germany, the use of vendors and other third parties in advertising—such as advertising agencies, DSPs, SSPs or data providers—is governed by the GDPR, supplemented by national provisions such as the BDSG, the UWG, and the TDDDG. See, generally, the European Union chapter. In addition, note that where vendors use cookies or similar technologies for tracking and targeting purposes, prior consent is required under the TDDDG. Further care must be taken to comply with the requirements of the TDDDG for end-user device access, and with the stricter interpretation of lawful advertising practices

under the UWG. Regulatory guidance from the Conference of Independent Data Protection Authorities of Germany ('DSK') reinforces the need for clear contractual arrangements, transparency, and valid user choices in third-party advertising setups.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

In Germany, companies disclosing or receiving personal data from vendors or other third parties in the context of advertising must comply with the GDPR, complemented by national requirements under the BDSG, the TDDDG, and relevant case law. See, generally, the European Union chapter.

Note, in particular, that the German supervisory authorities regularly stress the need for clear contractual allocation of responsibilities and minimum security standards. In the German context, additional attention must be paid to compliance with the TDDDG, where data access occurs on or through end-user devices. Even if no personal data is processed in the GDPR sense, consent and transparency requirements under the TDDDG may still apply and must be reflected in contractual arrangements—particularly in the context of advertising technologies, measurement tools, and cross-site tracking.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

In Germany, companies are expected to take a range of organizational and legal steps to ensure that processing of personal data for advertising purposes complies with the GDPR, the BDSG and, where applicable, the TDDDG. This includes both general due diligence obligations and specific requirements when high-risk processing activities are involved. See the European Union chapter.

In Germany, supervisory authorities (through the DSK) have published additional guidance listing advertising-related scenarios where DPIAs are typically required—eg behavioral advertising using third-party trackers. Companies must regularly review and update their risk assessments in light of evolving technologies and regulatory expectations.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

In Germany, direct marketing via email, SMS, or push notifications is governed not only by the GDPR, but also by national legislation—most notably the UWG and the TDDDG. The legal framework is particularly strict and includes the following core requirements:

- (a) **Prior consent requirement:** Direct marketing via electronic communication channels generally requires prior, express and informed consent. The German courts and regulators consistently require a double opt-in process to demonstrate valid consent.
- (b) **Exception for existing customer relationships:** Marketing to existing customers may be permissible without additional consent if the company:
 - (i) obtained the contact data in connection with a sale,
 - (ii) uses it for advertising similar products or services,
 - (iii) informs the customer clearly of the right to object at the time of data collection, and
 - (iv) offers an easy opt-out in every message.

This is a narrowly interpreted exception.

- (c) **Right to object:** Data subjects have the right to object at any time to the use of their data for direct marketing. Upon objection, the processing must stop immediately and without exception.
- (d) **Identification and transparency obligations:** Marketing messages must clearly identify the sender, provide contact details, and include a simple and effective opt-out mechanism. Hidden identities or pre-ticked boxes are unlawful.
- (e) **Consent under the TDDDG:** Where marketing involves access to information on a user's terminal device (eg, push notifications enabled via app permissions), separate consent under the TDDDG is required unless the message is technically essential.

German regulators, particularly the regional DAPs and competition authorities, take an active role in enforcing compliance. Breaches may result in both administrative fines under the GDPR and injunctions or penalties under the UWG.

7.2 **How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?**

In Germany, the use of tracking technologies such as cookies, tracking pixels, SDKs, or similar tools is subject to both the GDPR and the TDDDG. The legal framework combines data protection principles with specific rules for device-level access. See the European Union chapter. Note, in respect of Germany, that consent is typically obtained via a consent management platform ('CMP'), and the German authorities have made clear that pre-checked boxes or bundled consents do not meet the legal requirements.

German supervisory authorities (notably the DSK and regional DPAs) are active in auditing cookie banners and have imposed fines for non-compliant practices. Practical enforcement has focused on dark patterns, non-functional opt-outs, and excessive default tracking.

7.3 **How are loyalty programs and promotions regulated under privacy law?**

In Germany, the operation of loyalty programs and promotional campaigns involving personal data must comply with the GDPR, supplemented by national rules under the BDSG, the UWG, and the TDDDG. Such programs often include personalized advertising, profiling, and tracking, which require particular care in implementation. See the European Union chapter. In practice, German regulators scrutinize loyalty schemes for transparency, lawful profiling, and compliant consent management.

7.4 **How is social media and influencer marketing regulated under privacy law?**

In Germany, social media and influencer marketing involving personal data processing must comply with the GDPR. See the European Union chapter. It is also shaped by national rules on advertising transparency (eg, UWG and case law), platform-specific policies, and the TDDDG where tracking is involved. In particular:

- (a) **Tracking and targeting tools:** Where social media marketing relies on cookies, pixels, or SDKs—such as Meta Pixel or TikTok tracking—consent must be obtained under the TDDDG. This applies regardless of whether the influencer or the brand operates the website or app involved.
- (b) **Advertising disclosure duties:** Separate from data protection, influencers must clearly label promotional content as advertising under competition law (notably the UWG and relevant case law of the BGH). Failure to do so may constitute misleading commercial practice, regardless of privacy compliance.

- (c) **Opt-out and control options:** Users must be able to withdraw consent or object to targeting and profiling activities. Where social media platforms act as independent controllers, influencers and brands should ensure users are appropriately directed to those mechanisms.

German regulators closely monitor influencer marketing—both from a privacy and competition perspective.

7.5 **How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

In Germany, targeted advertising—particularly when based on user behavior or profiling—is subject to the full scope of the GDPR (for which see the European Union chapter) as well as specific national rules under the TDDDG and the UWG. By contrast, contextual advertising is generally considered low-risk from a privacy perspective and subject to more limited obligations. Note the following:

- (b) **Consent under the TDDDG:** The use of tracking technologies (eg third-party cookies, pixels, SDKs) for advertising purposes constitutes access to or storage of data on a user's device. Except where technically necessary, this always requires separate consent in accordance with the TDDDG.
- (c) **Profiling and data sharing:** Where advertising involves profiling or enriched targeting through data brokers or ad tech intermediaries, organizations must be transparent about the logic behind the targeting, the categories of data used, and whether automated decision-making takes place. Additional safeguards may be necessary if the outcome significantly affects the individual (eg price variation, exclusion from offers).
- (e) **Regulatory guidance and enforcement:** The German supervisory authorities have repeatedly clarified that consent must be obtained before tracking for advertising purposes begins, and that 'cookie walls' without real alternatives are not valid. Enforcement efforts have focused on insufficient or deceptive consent mechanisms, undisclosed third-party tracking, and unlawful profiling.

7.6 **How are digital identity resolution and clean room technologies regulated under privacy law?**

In Germany, the use of digital identity resolution tools and clean room technologies is subject to the GDPR (for which see the European Union chapter) and further shaped by national requirements under the TDDDG and the BDSG. These technologies often involve combining or linking data sets across systems or parties for advertising and analytics purposes, raising particular concerns around transparency, lawful processing, and data minimization.

Supervisory authorities in Germany are increasingly reviewing these practices in light of recent developments in adtech and data collaboration models.

7.7 **How is location-based advertising regulated under privacy law?**

In Germany, location-based advertising is regulated under the GDPR (for which see the European Union chapter) and the TDDDG, given that location data qualifies as personal data when it relates to an identifiable individual or device. The use of such data for marketing purposes requires strict compliance with both legal and technical safeguards. In particular, note that if the location data is obtained via terminal equipment (eg mobile apps or browser-based tools), separate consent under the TDDDG is required unless the tracking is strictly necessary for a core service explicitly requested by the user. This applies even if no personal data is processed.

German regulators increasingly monitor mobile marketing practices and have stressed in guidance that location data is highly sensitive and often entails significant risks to user privacy.

7.8 How are data brokers defined and regulated under privacy law?

In Germany, data brokers—typically companies that aggregate, enrich, and trade in personal data without a direct relationship to the data subjects—are fully subject to the GDPR, as well as to enhanced transparency expectations under national enforcement practice. While the term ‘data broker’ is not legally defined, their business model falls under the standard rules for controllers. See the European Union chapter.

Note that supervisory authorities in Germany—particularly in Berlin, Hamburg, and Bavaria—have initiated proceedings against companies operating opaque data aggregation models, focusing on the failure to provide notice and the lack of clarity about data sources.

While data brokerage is not prohibited per se, companies in this sector are required to demonstrate a high degree of accountability, maintain records of processing activities, and be able to respond effectively to access and erasure requests.

7.9 How is advertising to children and minors regulated under privacy law?

In Germany, advertising that targets children or adolescents is subject to heightened legal scrutiny under the GDPR, complemented by national norms and regulatory guidance that emphasize protective standards for underage individuals. This applies particularly to online environments, apps, and digital media platforms aimed at younger audiences:

- (a) **Age threshold and consent:** For advertising addressed to children under 16, the GDPR requires verifiable parental consent when personal data is processed—eg for personalized ads or behavioral tracking. Germany has not lowered the threshold below 16, unlike some other EU states.
- (b) **Child-appropriate transparency:** Privacy notices and consent interfaces must be formulated in a manner understandable to the target age group. This includes simplified language, clear iconography, and avoiding misleading design (‘dark patterns’) that might pressure young users into agreeing.
- (c) **Profiling and behavioral targeting:** Profiling for advertising purposes involving children is strongly discouraged in German regulatory practice. If it is carried out, controllers must apply strict safeguards, justify the necessity, and ensure the outcome does not adversely affect the child’s interests.
- (d) **Tracking technologies and terminal access:** The use of cookies, app SDKs, or pixels for targeting minors triggers prior consent requirements under the TDDDG, irrespective of whether the minor fully understands the technology. Consent from the child alone is invalid where parental consent is legally required.
- (e) **Principle of fairness and protection of minors:** The GDPR’s fairness principle is interpreted particularly strictly in relation to minors. Advertising strategies must not exploit the inexperience or emotional vulnerability of children. In addition, the German Interstate Treaty on the Protection of Minors in the Media may impose content-based restrictions.

Regulatory authorities in Germany expect that child-focused services incorporate data minimization, strong default privacy settings, and age-appropriate consent mechanisms.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

In Germany, the use of profiling, AI systems, and automated decision-making for advertising is governed by the GDPR and subject to strict standards concerning fairness, accountability, and individual control. See the European Union chapter. German authorities apply these rules with particular attention to transparency and power asymmetries in digital advertising environments.

The principle of fairness under the GDPR is reinforced in German guidance with emphasis on avoiding manipulation, particularly in vulnerable groups. Where profiling or algorithmic decision-making is used to personalize content, target ads, or segment users, organizations must inform individuals about the logic involved, the purpose, and the consequences of such processing. Supervisory authorities insist on concrete explanations, not abstract technical references.

The German data protection authorities actively monitor AI use in marketing, including adtech ecosystems and data enrichment services.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Yes, in Germany, cross-border data transfers require not only compliance with the GDPR but must also take into account additional national considerations—particularly in legally sensitive contexts such as regulated professions, litigation, and public sector data handling:

- (a) **Professional secrecy and privilege:** Certain sectors (eg, legal, medical, tax advisory) are subject to statutory confidentiality obligations under national law. If personal data subject to professional secrecy is transferred to third countries, especially outside the EEA, such transfers may be unlawful if adequate confidentiality safeguards are not contractually and technically ensured. In practice, this limits outsourcing to non-EEA jurisdictions in law firms or medical IT systems.
- (b) **Public sector constraints:** Public authorities in Germany face stricter transfer rules, including under the BDSG, which may require explicit legal authorization for international transfers.
- (c) **Judicial and regulatory cooperation:** Transfers for litigation, arbitration, or regulatory cooperation (eg antitrust or tax investigations) must consider both the GDPR (necessary for legal claims) and national procedural rules on data handling and evidence transfer.
- (d) **Transfer Impact Assessments (“TIA’s”):** Following Schrems II, German data protection authorities expect detailed TIAs before using tools or services involving third-country transfers—especially where surveillance concerns exist. In certain cases, they have warned against using US-based providers without strong encryption and contract clauses.

- (e) **Sector-specific restrictions:** Certain industries (eg insurance, finance, health) are governed by additional laws which may further restrict or condition international data flows—especially where sensitive or large-scale data processing is involved.

In summary, transfers from Germany must be evaluated not only under the GDPR but also in light of confidentiality laws, sector-specific regulations, and supervisory expectations. This layered approach requires both legal and operational due diligence, particularly where privileged or high-risk data is involved.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Germany? Are there minimum standards? Does this differ by sector or size of the entity?

In Germany, data security is primarily governed by the GDPR, which obliges all controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures must take into account the state of the art, implementation costs, the nature of the data, and the potential impact on the rights of individuals. Note that:

- (a) The GDPR does not prescribe fixed technical requirements but demands a risk-based approach. However, in Germany, the Federal Office for Information Security ('BSI') provides non-binding but widely used technical standards, such as the BSI IT-Grundschutz Catalogues, which are commonly applied to assess compliance in practice.
- (b) Certain sectors are subject to additional statutory security obligations under the BSI Act. Operators of so-called 'critical infrastructures'—including energy, health, transport, and finance—must implement state-of-the-art security measures, report serious incidents to the BSI, and undergo regular audits. Since 2023, these obligations have been expanded under the IT-Sicherheitsgesetz 2.0.
- (c) While the GDPR applies to all entities regardless of size, larger organizations or those with risk-prone processing activities (eg behavioral advertising, health data, children's data) are expected to adopt more advanced and documented security measures, including access control, encryption, and incident response plans.
- (d) German supervisory authorities expect documented security concepts and risk assessments. In data breach investigations, insufficient technical or organizational security can lead to substantial fines—even if no breach actually occurred.

9.2 How are personal data breaches regulated in Germany? What are the requirements for notification and response?

In Germany, the handling of personal data breaches is governed by the GDPR and further shaped by the BDSG as well as by detailed guidance from German supervisory authorities. Timely response, documentation, and risk assessment are key elements of compliance. Note that:

- (a) A controller must notify the competent data protection authority—typically the authority of the federal state concerned—within 72 hours of becoming aware of a personal data breach, unless it can be reasonably assumed that the breach poses no risk to the rights and freedoms of affected individuals. The notification must describe the nature of the breach, categories of data and data subjects involved, likely consequences, and mitigation measures taken.

- (b) If the breach is likely to result in a high risk, individuals must be informed without undue delay. The message must be in clear and plain language and explain the nature of the breach and recommended protective steps.
- (c) Whether notification is required depends on the risk level. For example, accidental deletion of encrypted backup data may not trigger reporting, while unencrypted leaks of health or location data would generally require full notification.
- (d) All breaches must be documented internally, regardless of whether notification is required. The record should include details of the incident, risk assessment, and remedial actions, and must be available for inspection by the authority upon request.
- (e) Supervisory authorities expect prompt and well-documented incident handling, including evidence of breach detection procedures, internal communication protocols, and remediation steps. Failures to report within the deadline or underestimation of risk have led to significant fines.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In Germany, enforcement of privacy laws—particularly concerning advertising practices—has intensified, with both regulatory authorities and courts actively addressing non-compliance. This includes significant fines, legal actions, and evolving litigation trends. In particular:

- (a) **Regulatory enforcement:** German data protection authorities ('DPA's) have been proactive in enforcing GDPR compliance, especially in the advertising sector. For instance, the Berlin DPA imposed a €14.5 million fine on a real estate company for inadequate data deletion practices, highlighting the importance of data minimization and storage limitation principles. Additionally, the North Rhine-Westphalia DPA has emphasized the necessity for clear consent mechanisms in online advertising, particularly concerning cookie usage and tracking technologies.
- (b) **Judicial actions and litigation trends:** German courts have seen a rise in privacy-related litigation, including cases involving advertising practices. Notably, the Federal Court of Justice ruled that even a brief loss of control over personal data could warrant non-material damages under the GDPR, setting a precedent for future claims.
- (c) **Privacy matters:** Furthermore, the European Court of Justice ('CJEU') has clarified that competitors can bring actions against each other for GDPR violations under the Unfair Competition Act, potentially increasing litigation risks for companies engaged in advertising activities.

- (d) **Collective actions and consumer advocacy:** Consumer protection organizations in Germany, such as the Federation of German Consumer Organizations, have been active in scrutinizing data protection practices, particularly regarding online advertising and cookie consent. These organizations have initiated legal actions against companies for inadequate data protection notices and non-compliant consent mechanisms.

The enforcement landscape in Germany demonstrates a robust approach to ensuring compliance with privacy laws in advertising. Companies must prioritize transparent data processing practices, obtain valid consent for targeted advertising, and be prepared for potential regulatory scrutiny and litigation.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Germany?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

In Germany, several key developments in data protection and digital regulation are expected to shape the compliance landscape in the near future. Companies operating in advertising, digital services, or data-driven sectors should closely monitor the following emerging topics and legal challenges:

- (a) **DMA and DSA enforcement:** The Digital Markets Act (‘DMA’) and Digital Services Act (‘DSA’) are now in force, with Germany’s competition and media regulators playing an active role in implementation. Gatekeepers and online platforms face heightened scrutiny for profiling, recommender systems, and consent practices.
- (b) **Cross-border data transfers and TIAs:** Following Schrems II, German supervisory authorities continue to enforce strict expectations regarding international transfers. TIAs, supplementary measures for standard contractual clauses, and service provider audits remain a major compliance burden—especially in the context of US-based vendors.
- (c) **Consent management and dark patterns:** The correct design of CMPs is under increasing scrutiny. German authorities have issued warnings and guidance against manipulative user interfaces (eg, hidden opt-outs, pre-checked boxes), and enforcement in this area is expected to intensify.
- (d) **AI regulation and automated profiling:** With the forthcoming EU AI Act, companies must prepare for stricter regulation of algorithmic decision-making and advertising-related profiling. German authorities already require detailed justification and transparency where AI tools significantly affect users (eg, dynamic pricing or scoring).
- (e) **Non-material damages litigation:** Courts in Germany are increasingly receptive to claims for non-material damages under the GDPR. There is growing case law on what constitutes ‘emotional harm’ or ‘loss of control,’ and collective actions are expected to increase as procedural tools like the Consumer Rights Enforcement Act gain traction.
- (f) **Children’s data and youth-targeted advertising:** Authorities are paying closer attention to platforms and apps used by minors. Verifiable parental consent, age-appropriate privacy information, and content restrictions under the Interstate Treaty on the Protection of Minors in the Media are becoming more relevant.

- (g) **Data retention and deletion policies:** Several German DPAs have launched audits on data retention practices, particularly in Human Resources, Customer Relationship Management, and marketing systems. Companies should review deletion routines, system configurations, and documentation to avoid enforcement action.
- (h) **Employee data protection:** Ongoing reform discussions around data processing in the employment context may soon lead to updated rules on tracking, monitoring, and consent in the workplace—an area of high legal uncertainty.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, the privacy landscape in Germany and the broader EU has undergone significant changes, driven by regulatory, judicial, and technological developments. These shifts have tightened compliance expectations and broadened the scope of privacy law in practice. Key developments include:

- (a) **Post-Schrems II enforcement of international data transfers:** Following the CJEU's Schrems II ruling, German supervisory authorities have intensified their review of cross-border data flows, especially to the United States. This has triggered a surge in TIAs, contractual revisions using updated Standard Contractual Clauses ('SCCs'), and growing pressure to adopt EU-based service providers.
- (b) **Invalidation of consent mechanisms and focus on dark patterns:** Several German data protection authorities have declared common cookie banners and CMPs non-compliant, citing misleading design and lack of genuine user choice. This has led to heightened regulatory enforcement and stricter expectations for transparency and opt-in structures.
- (c) **Introduction of the DSA and DMA:** These new EU regulations, applicable since 2023/2024, impose additional obligations on online platforms, particularly regarding profiling, recommender systems, algorithmic transparency, and advertising disclosures. They complement the GDPR but introduce distinct rules and enforcement pathways.
- (d) **Expansion of litigation under the GDPR:** Courts in Germany, including the Bundesgerichtshof, have clarified the thresholds for claiming non-material damages following data protection violations. This has contributed to a steady increase in private enforcement actions, often brought by consumer rights organizations or specialized law firms.
- (e) **Increased scrutiny of AI and profiling practices:** Anticipation of the EU AI Act and growing attention to algorithmic targeting have led to more regulatory inquiries into profiling, scoring, and automated decision-making—especially in the advertising and HR sectors.
- (f) **Focus on children's privacy and youth-targeted services:** In response to EU-wide trends and media scrutiny, German regulators have increasingly prioritized child-specific consent mechanisms, age-appropriate privacy information, and advertising restrictions in digital environments aimed at minors.

These developments were triggered by a combination of court decisions (notably from the CJEU and German civil courts), regulatory pressure from national DPAs and the European Data Protection Board, as well as EU legislative initiatives under the Digital Strategy framework.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies in Germany face growing complexity in privacy compliance due to evolving legal, regulatory, and technological developments. Key challenges include:

- (a) **International data transfers:** Ongoing uncertainty following Schrems II and strict expectations for TIAs and supplementary safeguards make global data flows legally and operationally demanding.
- (b) **Consent management and tracking:** Strict interpretation of consent under the GDPR and the TDDDG, combined with enforcement against dark patterns, has raised the bar for valid cookie and tracking practices.
- (c) **Increasing litigation risk:** Expanded use of the right under the GDPR to compensation for individuals and consumer organizations has led to more lawsuits and higher exposure to non-material damage claims.
- (d) **Sector-specific obligations:** Entities in health, finance, and critical infrastructure face overlapping requirements under the GDPR, the BDSG, the BSI Act, and sectoral laws—often requiring parallel compliance strategies.
- (e) **AI, profiling, and upcoming EU legislation:** The anticipated EU AI Act and growing regulatory scrutiny of algorithmic decision-making require companies to reassess profiling practices, particularly in advertising and HR.

12.3 What do you envision the privacy landscape will look like in five years?

In five years, privacy regulation in Germany is expected to become more integrated, sector-specific, and enforcement-driven. Key developments will likely include:

- (a) **Consolidated EU digital regulation:** The GDPR will operate alongside fully implemented frameworks like the AI Act, DMA, DSA, and ePrivacy Regulation, creating a layered and interconnected compliance regime.
- (b) **Stronger enforcement and litigation:** Supervisory authorities will likely increase coordination and impose higher fines, while collective actions and damage claims under Article 82 GDPR will become more common.
- (c) **Technical accountability:** Companies will be expected to embed privacy deeply into design and governance—particularly for AI, cross-border processing, and automated decision-making.
- (d) **Risk-based sector regulation:** Privacy obligations will increasingly reflect the sensitivity and context of data use, with stricter rules in health, finance, and digital advertising.

Germany will remain one of the most stringent enforcement environments in the EU, with high standards for transparency, consent, and data minimization.

 GREECE 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Greece.

Privacy in Greece is, first of all, protected at a constitutional level, by the Greek Constitution, which provides that: ‘All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.’

Furthermore, the protection of personal data is specifically regulated in Greece; primarily, by European Law and, complementarily, by national law.

More specifically, as in all EU Member States, the primary source of privacy law in Greece is the General Data Protection Regulation 2016/679 (‘GDPR’) (see the European Union chapter).

Additionally, national Law No 4624/2019 (‘Greek Data Protection Law’) sets some rules regarding the implementation of certain aspects of the GDPR in Greece, in relation to which the GDPR contains opening clauses. These national rules either specify or limit some of the rights and obligations provided by the GDPR.

Privacy rules in the electronic communications sector are also set by Greek Law No 3471/2006 (as amended), which implemented the ePrivacy Directive.

1.2 What are the primary laws regulating privacy in Greece? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy in Greece is mainly regulated by the GDPR, which came into force, as in all Member States, on May 25, 2018 and is directly applicable in Greece, with no need of incorporation by the national legislator (see the European Union chapter).

Additionally, the Greek Data Protection Law, which entered into force on August 29, 2019, sets specific provisions regarding the implementation of certain aspects of the GDPR in Greece, and also incorporates the EU Law Enforcement Directive (2016/680) into Greek law.

The most important provisions relating to private entities in the Greek Data Protection Law, which are supplemental to the provisions of the GDPR, concern:

- (a) consent of minors to processing of their personal data in relation to information society services (see question 3.2);
- (b) processing of special categories of personal data for certain purposes other than those provided in the GDPR (see question 3.2);
- (c) prohibition on processing of genetic data for purposes of health and life insurance (see question 3.2);
- (d) processing of personal data for further purposes other than those for which the data had been collected;
- (e) processing of personal data in the context of employment;
- (f) processing of personal data in specific situations, such as academic, artistic or literary expression and journalistic purposes, scientific or historical research purposes, or for the collection or retention of statistics;

- (g) exceptions from the obligation to inform data subjects; exceptions to the right of access and to the right of erasure; and release from the obligation to communicate a data breach to the data subject in specific cases ; and
- (h) penal sanctions for specific willful violations of data protection law.

The Greek Data Protection Law has also repealed Greek Law No 2472/1997 (which had been the main legislative text regulating protection of personal data in Greece prior to the GDPR), with the exception, however, of certain specific provisions which still remain in force, such as the right of data subjects to declare to the Hellenic Data Protection Authority that they do not want their personal data to be processed by anybody for purposes of marketing communication by post.

In addition, especially in relation to the protection of privacy in the electronic communications sector, Greek Law No 3471/2006 provides rules for marketing communications by electronic means.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Advertising self-regulation has gained much importance in Greece in recent years. The main self-regulation organization in Greece is the Advertising Self-Regulation Council ('SEE') which is a member of the European Advertising Standards Alliance ('EASA') and enforces the Hellenic Code of Advertising and Communication Practice ('HCACP').

The structure and content of the HCACP is almost identical to the ICC Consolidated Code of Advertising and Communication Practice. The HCACP covers both non-broadcast and broadcast advertising, including online advertising and social media. The HCACP sets forth specific provisions on the protection of personal data and privacy. The HCACP also has a special Chapter on direct marketing and digital marketing communications, which includes privacy-related provisions.

SEE may be activated either after an ex officio monitoring or after submission of a written complaint. Both consumers and competitors are entitled to file complaints claiming that a marketing communication breaches the HCACP.

However, as noted in the European Union chapter, self-regulation is only a supplementary mechanism in relation to enforcing privacy rules. The main authority responsible for monitoring compliance with privacy law in Greece is the Hellenic Data Protection Authority ('Hellenic DPA'), which is an independent supervisory authority (see question 1.4).

1.4 How is privacy law enforced in Greece? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The independent supervisory authority responsible for monitoring the implementation and enforcement of privacy law in Greece is the Hellenic DPA. The Hellenic DPA has the competency, inter alia, to handle complaints, investigate possible breaches of privacy law, issue decisions and impose administrative sanctions (including monetary fines) in cases of violation of data protection rules.

In addition, data subjects who wish to seek compensation or other form of restitution in cases of unlawful processing of their personal data by a controller or processor, may bring civil actions before the competent civil courts, which will, in this case, also enforce privacy law.

Furthermore, in cases of penal violations in relation to personal data, which are specifically provided in the Greek Data Protection Law, the penal courts are also competent to enforce the data protection rules.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Greece?

As far as the GDPR is concerned, please see the European Union chapter.

The Greek Data Protection Law applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, by public or private bodies, with the exception of processing of personal data by a natural person in the course of a purely personal or household activity. 'Private bodies' are considered to be all natural or legal persons or associations of persons without legal personality, that do not fall within the definition of 'public bodies'. Thus, as is the case with the GDPR, all companies fall under the obligations of the Greek Data Protection Law, subject only to its territorial scope (see question 2.2).

2.2 Does privacy law in Greece apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, Greek privacy law can apply to companies outside Greece.

As far as the GDPR is concerned, please see the European Union chapter.

The Greek Data Protection Law applies to private bodies when:

- (a) a controller or processor processes personal data in Greece, or
- (b) personal data is processed in the context of the activities of an establishment of a controller or a processor in Greece, or
- (c) even if the controller or the processor does not have an establishment in the EU/EEA, they fall within the scope of the GDPR.

In cases where a controller or processor, who falls under the scope of the law, is established outside the EU, they should designate a representative in writing (please see the European Union chapter).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Greece?

The GDPR definition applies (see the European Union chapter). There is no different definition of 'personal data' in the Greek Data Protection Law.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

Also, in relation to the 'special categories of personal data', the Greek Data Protection Law exceptionally permits private bodies to process such categories of personal data, if the processing is necessary:

- (a) to exercise rights derived from the right of social security and social protection and to meet the related obligations; or

- (b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, for medical diagnosis, for the provision of health or social care or treatment or for the management of health or social care systems and services, or pursuant to the data subject's contract with a health professional or other person who is subject to the obligation of professional secrecy or is under their supervision.

In the above cases, of course, appropriate and specific measures need to be taken to safeguard the interests of the data subject.

In addition, processing of genetic data for purposes of health and life insurance is prohibited.

With regards to personal data of children, the Greek Data Protection Law provides that, when consent is the legal basis for processing of non-sensitive personal data of children in relation to information society services, a child should be at least 15 years old in order to give valid consent. If the minor is below the age of 15, the consent of the person holding parental responsibility is required.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter. Also, see question 1.2 in relation to limitations of data subjects' rights provided by the Greek Data Protection Law.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

Also, the Hellenic DPA has issued a list of processing activities for which it considers that it is obligatory to carry out a data protection impact assessment ('DPIA'). The list, inter alia, includes cases of systematic data processing for marketing purposes which involve profiling of natural persons, when the data are combined with data collected from third parties.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for privacy law obligations.

In addition:

- (a) With regard to marketing communications through electronic means, such as by email, SMS, fax, automated calls, etc (with the exception of calls made with human intervention), it is necessary, as a general rule, that the receiver of the communication/data subject has provided valid, informed and explicit consent prior to the communication ('opt-in' system). In a decision in 2022, the Hellenic DPA deemed that the same requirements also apply when sending marketing communications to an email address belonging to a legal entity.

Nevertheless, in cases where the electronic contact details have been previously acquired legally in the framework of a commercial relationship with the data subject (eg, previous sale of products or provision of services to the data subject), it is possible to use such data for future marketing communication in relation to similar products or services, even if the recipient of the communication had not provided prior explicit consent (it is noted that in a decision in 2022, the Hellenic DPA ruled that being 'connected' with the data subject on LinkedIn does not suffice in order to add the data subject's email to a newsletter recipient list without consent). However, it is absolutely necessary to provide, both when the data is collected as well as in each communication, a clear, easy and free way for data subjects to

object to the collection and use of their contact details in the future ('soft opt-in' system). In a decision in 2019, the Hellenic DPA imposed a fine of €200,000 on a leading Greek telecommunications provider, because it was found that, starting from 2013, about 8,000 recipients of advertising emails were not able to successfully use the 'unsubscribe link' provided in the emails in order to object to receiving the provider's further marketing communications, due to a technical error that had not previously been detected. This situation was deemed by the Hellenic DPA to be in violation of the right of data subjects to object to processing for direct marketing purposes, as well as to the principle of privacy by design, provided by the GDPR.

- (b) Regarding phone calls made with human intervention for direct marketing purposes, consumers have the right to declare, for free, to their telecommunication provider that they do not wish to receive this kind of marketing calls ('opt out' system). Each telecommunication provider has the obligation to keep a registry of the subscribers who have provided this declaration; and any interested party who wishes to make direct marketing calls should previously check the registries kept by each provider and comply with them. In relation to this matter, the Hellenic DPA in 2019 imposed a considerable administrative fine of €200,000 on a leading Greek telecommunications provider for not keeping the registry provided to advertisers properly updated. This resulted in phone calls to subscribers who had opted out of this kind of direct marketing. The incident was found by the Hellenic DPA to infringe the principle of accuracy and to the principle of data protection by design, provided by the GDPR.
- (c) The Hellenic DPA also keeps a registry of data subjects who do not wish to receive marketing communications by traditional post. It is a legal obligation for data controllers to check this opt-out registry prior to sending such marketing communications.
- (d) In relation to marketing communications through the Viber app, in 2018, the Hellenic DPA issued a decision which provides some guidance to private companies (data controllers). According to this decision, the lawfulness of sending Viber messages for direct marketing purposes can be based either on the consent of the data subject or on the legitimate interests of the data controller. In addition, the Hellenic DPA considered that accepting to receive such messages from the data controller through the 'Viber business' service did not constitute valid consent, since it did not meet the criteria in the Greek privacy law in force at the time, nor the GDPR. This is because the data subject was not properly informed of the purpose of the processing (namely the promotion of products/services of the company) during the collection of the data; nor was the purpose of sending the message adequately defined at the point of sending.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

- 7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

See the European Union chapter.

- 7.6 How are digital identity resolution and clean room technologies regulated under privacy law?**

See the European Union chapter.

- 7.7 How is location-based advertising regulated under privacy law?**

See the European Union chapter.

- 7.8 How are data brokers defined and regulated under privacy law?**

See the European Union chapter.

- 7.9 How is advertising to children and minors regulated under privacy law?**

The Greek Data Protection Law provides that, when consent is the legal basis for the processing of non-sensitive personal data of children in relation to information society services, a child should be at least 15 years old in order to give valid consent. If the minor is below the age of 15, the consent of the person holding parental responsibility is required.

See also the European Union chapter.

- 7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?**

See the European Union chapter.

- 7.11 Are there other specific advertising practices that you wish to discuss?**

See question 11.2 in relation to ‘dark patterns’.

8 DATA TRANSFERS

- 8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?**

See the European Union chapter.

- 8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?**

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Greece? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

9.2 How are personal data breaches regulated in Greece? What are the requirements for notification and response?

See the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter regarding the administrative sanctions.

In addition, the Greek Data Protection Law provides also penal sanctions for specific willful violations of data protection law.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter. See also our answer to question 1.4 above.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In recent years, the Hellenic DPA has handled a number of cases that involve advertising, especially regarding issues of direct marketing by email, SMS or phone calls. The sanctions issued, if GDPR violations are found, are determined on a case-by-case basis. See, for example, question 7.1, in relation to two considerable administrative fines, each amounting to €200,000, that were imposed on a leading telecommunications provider in Greece in relation to issues of direct marketing.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Greece?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

The prohibition on 'dark patterns' is a topic that companies should be aware of, especially in relation to online marketing and online tracking methods. Depending on the case, dark patterns may violate various legal provisions, and especially consumer protection and data protection laws.

In relation to privacy, dark patterns may particularly infringe the rules for legitimately obtaining a person's informed consent, as well as the legal principles of transparency, privacy-by-design and privacy-by-default. In this context, the European Data Protection Board has also adopted Guidelines on 'deceptive design patterns in social media platform interfaces'.

It is also noted that, for cases not covered by legislation on consumer protection or data protection, the EU Digital Services Act ('DSA') expressly sets a 'ban' on dark patterns in online platforms, by prohibiting the platforms from designing, organizing or operating their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs a user's ability to make free and informed choices. In addition to the DSA, the Digital Markets Act ('DMA'), the Data Act and the AI Act also contain provisions that prohibit specific dark patterns.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Hellenic DPA has issued rather heavy administrative fines to companies in cases of major violations of the GDPR. For example:

- (a) In July 2022, the Hellenic DPA imposed a fine of €20 million on a very well-known American facial recognition company for various GDPR violations, and ordered it to not collect and process personal data of data subjects located in Greece by using facial recognition technology, and to delete any data already collected.
- (b) Regarding data breaches, in January 2022, the Hellenic DPA imposed very heavy fines of €9.25 million in total on a major Greek mobile operator and its parent company, a major telecommunications provider, for various GDPR violations related to the circumstances of a cyberattack that took place in 2020, which affected millions of data subjects.
- (c) Another considerable fine of almost €3 million was imposed in February 2024 on a leading postal service provider in Greece, following a cyberattack which resulted in the leakage of personal data on the dark web, because the Hellenic DPA deemed that the data controller had failed to implement appropriate technical security measures and to effectively apply policies regarding the protection of personal data.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

See the European Union chapter.

12.3 What do you envision the privacy landscape will look like in five years?

The decisions and guidelines that the Hellenic DPA issues over the years have a great importance for the interpretation and application of the GDPR in Greece; therefore, companies need to seek local legal advice in case Greek privacy rules apply.

 HUNGARY 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Hungary.

Privacy law is regulated by various Acts in Hungary. In addition to the EU General Data Protection Regulation ('GDPR'), which forms part of Hungarian law, there is a general Hungarian data protection act, namely, the Act on the Informational Self-Determination and the Freedom of Information ('Infotv').

The Infotv has several prongs. Amongst others, it contains rules due to the GDPR and, at the same time, transposes the EU Law Enforcement Directive (680/2016) into Hungarian law.

In addition to the GDPR and the Infotv, there are a number of sector-specific acts which contain provisions on data processing (see question 1.2).

As the GDPR is an EU Regulation which is directly effective and applicable in all Member States, including Hungary, no Hungarian Act may contradict the GDPR.

1.2 What are the primary laws regulating privacy in Hungary? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The main source of law for data protection is the GDPR, which is an EU Regulation directly effective and applicable in all EU Member States without any need for implementation whatsoever.

The GDPR contains around 90 opening clauses which allow Member States to either deviate from or supplement the provisions of the GDPR. Hungary has taken advantage of some of the opening clauses.

In addition to the GDPR and the Infotv, there are several pieces of legislation which contain provisions governing data processing. These include, for example:

- (a) the Hungarian Labor Code, and
- (b) the Whistle-blowing Act.

For details on the legal basis of processing in a marketing context, please see question 4.3 below.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Hungarian Advertising Code of Ethics was developed to serve as a set of professional and ethical guidelines for those involved in advertising activities in Hungary. It is widely recognized and adhered to within the industry. The Code incorporates various provisions related to privacy law. Both businesses and consumers have the right to approach the Self-Regulatory Advertising Board if they believe the Code has been violated. While the Board's decisions are not legally binding, they are typically respected and followed within the industry.

1.4 How is privacy law enforced in Hungary? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

In Hungary, there are no self-regulatory bodies in charge of the enforcement of privacy law.

The GDPR, the Infotv and all other laws on data processing are enforced by the National Data Protection and Freedom of Information Authority ('NAIH'). The NAIH regularly publishes resolutions on and uploads opinions and recommendations onto its website. Courts are also in charge of enforcement.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Hungary?

Taking the scope of the GDPR and the Infotv into account, all companies are subject to privacy law.

The scope of the Infotv is worded in such a way that the Act applies to the processing of personal data by a controller:

- (a) if the controller has its main establishment or only place of administration within the European Union in Hungary; and
- (b) where the controller has its main establishment or only place of administration within the European Union outside Hungary, but the data processing activities carried out by the controller, or the processor as per the instructions of the controller, are related to:
 - (i) the offering of goods or services to data subjects in Hungary, irrespective of whether a payment of the data subject is required, or
 - (ii) the monitoring of data subjects' behavior to the extent that their behavior takes place within Hungary.

The GDPR applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form (or is intended to form) part of a filing system. In this regard, it is worth noting that the Infotv provides that the rules of the GDPR also apply to the processing of data which do not form part of a filing system.

2.2 Does privacy law in Hungary apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. See question 2.1.

Controllers or processors not established in the European Union are required to designate a representative in the European Union in writing.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Hungary?

The GDPR contains a definition of personal data. Member States may not deviate from such definition and may not even duplicate the definition in their national laws as regards data processing activities covered by the GDPR.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The GDPR lists the special categories of personal data, and contains rules applicable to personal data relating to criminal convictions and offences. All such data can be regarded as being sensitive. Furthermore, even though, for example, financial or geo-location data do not qualify as special categories of personal data, they can be considered sensitive data, which is supported by the recitals of the GDPR and the practice of the European Data Protection Board ('EDPB', formerly known as the Article 29 Working Party or WP29) and the NAIH.

When it comes to the processing of special categories of data, the GDPR explicitly prohibits this unless certain strict prerequisites apply. When processing sensitive data under one of these exceptions, special obligations apply, which may include the need to prepare a data protection impact assessment ('DPIA') and to appoint a data protection officer ('DPO'). In addition, under the GDPR, there is a general obligation vested with the controller and the processor to take appropriate technical and organizational measures to safeguard the personal data and the rights and freedoms of data subjects. If sensitive data are also processed, the required level of security is higher.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

As regards data protection principles (including data minimization), information on data processing and the keeping of records of processing activities, the provisions of the GDPR have to be complied with. See the European Union chapter.

The same applies to the designation of a DPO, since Hungarian law contains no additional requirements in addition to those included in the GDPR.

As regards the preparation of a DPIA, the NAIH has issued a blacklist of data processing activities, which is a non-exhaustive list of those data processing activities that are subject to a DPIA. As per the list, we take it that, if profiling (eg, behavioral advertising) takes place, a DPIA has to be prepared prior to such data processing.

Internal data protection training is required, as controllers and processors are obliged to make sure that there is an adequate level of data protection awareness within their organization.

There is no obligation to register with the NAIH.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. Even though the GDPR applies to controllers and processors, there are certain obligations that only apply to controllers (eg, the obligation to prepare a DPIA if the conditions apply; the notification of a data breach to the competent supervisory authority and to the data subjects, if the conditions apply; and the documentation of data breaches). See the European Union chapter.

Hungarian law contains special provisions with regards to, eg, data retention periods which apply to controllers.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, a lawful basis is always required. For the rules of the GDPR, see the European Union chapter.

Under Hungarian law:

- (a) Postal marketing communications can be sent to data subjects based on their prior informed consent. If, however, the marketing material qualifies as a so-called 'addressed advertisement

parcel', it can be sent to the data subject based on the legitimate interest of the controller (opt-out regime). ('Addressed advertisement parcel' means a communication, consisting solely of advertising, marketing or publicity material and comprising an identical message, except for the addressee's name, address and other data which do not alter the nature of the message, which is sent to at least 500 addressees).

- (b) As to telephone calls, the Hungarian rules are as follows:
 - (i) personal calls: a subscriber may be called in the absence of any objection to receiving such calls (opt-out rule);
 - (ii) automated calls: the call is subject to the prior expressed consent of the subscriber (opt-in principle).
- (c) Emails or other kinds of electronic marketing communications are subject to the prior informed consent of the data subject.

In line with the GDPR, the NAIH stresses that no pre-checked boxes are allowed and that data subjects must be informed of the right to withdraw their consent or, if the data processing is based on the legitimate interest of the controller, the right to object.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The provisions of the GDPR apply. See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

The provisions of the GDPR apply. See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

For the lawful basis, please see question 4.3. Furthermore, the rules of the GDPR apply (eg, privacy policy, consent, legitimate interest assessment, DPIA).

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The provisions of the GDPR apply. See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The provisions of the GDPR apply. See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

The provisions of the GDPR apply. See the European Union chapter.

As regards the preparation of a DPIA, the NAIH has issued a blacklist of data processing activities, which is a non-exhaustive list of those data processing activities that are subject to a DPIA. As per the list, we take it that, if profiling (eg, behavioral advertising) takes place, a DPIA has to be prepared prior to such data processing.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See Sections 4 and 5 above.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See Sections 4 and 5 above.

7.3 How are loyalty programs and promotions regulated under privacy law?

See Sections 4 and 5 above.

7.4 How is social media and influencer marketing regulated under privacy law?

See Sections 4 and 5 above.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See Sections 4 and 5 above.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See Sections 4 and 5 above.

7.7 How is location-based advertising regulated under privacy law?

See Sections 4 and 5 above.

7.8 How are data brokers defined and regulated under privacy law?

See Sections 4 and 5 above.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter as to the GDPR and see Sections 4 and 5 above. We note that the processing of the personal data of children may not be based on the controller's legitimate interest.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See Sections 4 and 5 above.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The rules of the GDPR on data transfer apply. In addition to the rules of the GDPR, as a result of the CJEU's Schrems II decision, when transferring data to a third country (a non-EEA country), in addition to, eg, using signed standard contractual clauses, additional adequate guarantees have to be in place, including technical, organizational and contractual safeguards, ensuring an adequate level of protection to the personal data.

Furthermore, by way of example, the Whistle-blowing Act contains provisions on the restriction of data. The company to which the whistle-blowing report has been made is required to keep the data received confidential; only the persons taking part in the internal investigation may have access to the data and they may not transfer such data to any other person/unit of the employer.

In addition, other legislation, such as the Act on the Processing of Health Data, also contains rules applicable to data transfers.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

In addition to the rules of the GDPR and the consequences of the CJEU's Schrems II decision, companies need to consider whether sector-specific laws contain additional provisions on data transfer.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Hungary? Are there minimum standards? Does this differ by sector or size of the entity?

The provisions of the GDPR apply (ie, the controller and the processor are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk). This is a general, technology-neutral requirement which every entity falling within the scope of the GDPR is required to meet.

Furthermore, Hungary's Cybersecurity Act (which transposes the NIS2 Directive (2022/2555/EU) into Hungarian law) contains various obligations with which certain entities are required to comply (eg, registration with the supervisory authority, classification of electronic information systems, conduct of audits, appointment of a person in charge of information security matters, etc). The question of whether an entity falls under the scope of the Cybersecurity Act depends on, eg, the activities the entity carries out and the revenues and number of employees of the entity.

9.2 How are personal data breaches regulated in Hungary? What are the requirements for notification and response?

The provisions of the GDPR apply (eg, the controller is required to document data breaches and notify the data breach to the supervisory authority and the data subjects, if the conditions for such notifications apply). The implementation and effective operation of a proper incident response plan is essential.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The NAIH applies the sanctions as listed in the GDPR. Thus, depending on the circumstances of the case, the NAIH may, amongst other things:

- (a) issue reprimands to a controller or a processor where the processing operations have infringed provisions of the GDPR;
- (b) order the controller or the processor to comply with the data subject's requests to exercise their rights pursuant to the GDPR;
- (c) order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- (d) order the controller to communicate a personal data breach to the data subject;
- (e) impose a temporary or definitive limitation including a ban on processing;
- (f) impose an administrative fine; and
- (g) order the suspension of data flows to a recipient in a third country.

Under the GDPR, the maximum amount of the fine is €20 million, or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher. However, Hungary took advantage of the relevant opening clause of the GDPR to vary this, and the maximum fine that may be imposed on public authorities and bodies is set at HUF 20 million (about €49,250). This exception applies only to public authorities and bodies—not to entities other than public authorities and bodies to which entities the rules of the GDPR apply.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, under the GDPR individuals have the right to lodge a complaint with a supervisory authority and have the right to a judicial remedy against the controller or processor.

For example, data subjects may request the supervisory authority to order the controller to comply with their request (eg, right to access, right to erasure).

In addition, data subjects may claim compensation and/or a so-called 'harm fee' at court. When claiming a harm fee, no damages have to be proven, only the fact that an infringement of the data subject's right has taken place. It is worth noting that minor infringements will not result in any such harm fee becoming payable.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The NAIH has been very active in enforcing the provisions of the law. Direct marketing activities have historically been one of the main focus areas of the authority. The NAIH has imposed fines on various entities engaged in the conduct of direct marketing activities. Typically, the main violations are:

- (a) violation of data protection principles;
- (b) processing without a proper legal basis;
- (c) absence of a proper privacy policy; and
- (d) consent not obtained lawfully.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Hungary?

The Labor Code contains rules on the processing of biometric data and criminal data in the context of employment. In addition, it governs the control by the employer of the use of devices by their employees.

The Whistle-blowing Act contains mandatory rules governing when an entity sets up a whistle-blowing hotline scheme.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Entities wishing to apply AI-based solutions need to be cautious when it comes to setting up the framework for the use of such solutions, as certain data protection issues, as well as considerations under the EU AI Act, must be taken into account and properly addressed prior to the start of data processing.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The NAIH has so far issued several fines for the violation of the GDPR. The highest fine imposed was HUF 250 million (approx €616,000); this fine was imposed on a bank for unlawfully using AI. Typically, the fines imposed range between HUF 5 million (approx €12,315) and HUF 20 million (approx €49,250) and they have typically been imposed for the violation of a data subject’s rights, lack of transparency (lack of giving proper information), the violation of data protection principles, and the improper handling of data breaches.

The NAIH is in the practice of issuing opinion papers and recommendations. The documents are available on the website of NAIH. Also, the resolutions of NAIH are also uploaded on its website and some of the resolutions also name the entity against which a sanction has been imposed.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The EU's new network and information security directive ('NIS2 Directive') has been transposed into Hungarian law (see question 9.1). As regards the implementation of the NIS2 Directive, besides the Act transposing the Directive, several decrees have been adopted.

Hungary has implemented the EU's Whistleblowing Directive, which contains data processing rules with which entities falling under the scope of the Hungarian Whistleblowing Act are required to comply.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenge for companies is to think in a data protection and data security compliant way and to get used to the idea of taking data protection and data security rules into account at the appropriate stages of their operation (eg, when they are about to decide about an activity which necessarily means the processing of personal data).

In our experience, the giving of a proper data privacy notice to data subjects still causes difficulty for a number of controllers. The handling of data breaches is also an issue for many of them, as is the handling of data subjects' requests. Also, it seems that a number of companies lack a proper incident response plan and certain other documentation (eg, balancing tests when the processing is based on the legitimate interest of the controller or a third party; internal policies related to data processing, including, eg, a CCTV policy, or policy on the monitoring by the employer of electronic devices used by employees for work purposes, etc).

It is also worth noting that the data-related landscape is an ever-changing and a more and more challenging one, causing companies to struggle with various issues around data protection and data and information security.

12.3 What do you envision the privacy landscape will look like in five years?

As a result of the EU Member States' data protection authorities' continuous efforts to ensure effective enforcement of the GDPR and data protection laws, companies will likely tend to become more cautious about data protection issues and will put more focus on ensuring that their data processing operations are transparent and comply with applicable data protection laws.

AI and information security related laws will be more and more in the focus of many companies (and authorities alike).

 IRELAND 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Ireland.

As a common law system, all Irish laws are regulated by a mixture of statute (including EU directives) and judge-made case law. The primary authority regulating privacy in Ireland is the Data Protection Commission. It is governed by a number of legislative frameworks, primarily the General Data Protection Regulation ('GDPR') and the Data Protection Act 2018, both of which are discussed in further detail below.

Ireland was traditionally quite proactive in the area of privacy regulation, and the original legislation dates back to the Data Protection Act 1988. Some parts of the Data Protection Acts 1988 and 2003 were retained by the Data Protection Act 2018 and can still apply, particularly where a complaint relates to breaches which occurred prior to the commencement of the GDPR on May 25, 2018.

Since May 25, 2018, the primary regulatory framework is the GDPR. As discussed in the EU chapter, it has general application to the processing of personal data in the European Union, providing for wider obligations on data controllers and processors and offering a higher level of protection for data subjects. Although the GDPR had direct effect throughout the European Union, the Irish Data Protection Act 2018 was enacted to give effect to the GDPR in areas where Member States could give further effect to certain provisions, or had flexibility (for example, the GDPR allowed Member States to provide their own minimum digital age for consent).

The Data Sharing and Governance Act 2019 introduced requirements for the sharing of information, including personal data, between public bodies, provided for the establishment of base registries and the Personal Data Access Portal, and established the Data Governance Board.

Aside from the legislation highlighted above, Ireland is a common law system and privacy can also therefore be regulated by court decisions.

Even prior to the enactment of the GDPR, Ireland had perhaps seen more activity than many EU countries regarding data privacy, as many of the leading global social media and information technology multinationals use Ireland as their European base.

1.2 What are the primary laws regulating privacy in Ireland? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary law is the GDPR. It is directly applicable throughout the European Union and, therefore, from May 25, 2018 has regulated privacy in Ireland. Additionally, the Data Protection Act 2018 acts as secondary legislation. The Data Protection Act 2018 enacted additional provisions where flexibility was permitted under the GDPR and also formally established the office of the Data Protection Commission.

Marketing information and processing of personal data for advertising or marketing is governed by the GDPR and the Data Protection Act 2018, and does not have specific legislation. The Consumer Protection Act 2007 applies also to marketing practices if they are seen to be unfair; so, in theory, that could also be applied to a privacy complaint deriving from an unfair commercial practice.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation is an important part of the Irish regulatory sphere, particularly in relation to advertising. The GDPR and any local legislation would have primary importance, but the Advertising Standards Authority in Ireland ('ASA') also publishes a *Code of Standards for Advertising and Marketing Communications in Ireland* which is of importance for advertisers seeking to comply with privacy regulations. As a general principle of the Code, the ASA draws attention for advertisers to the importance of compliance with EU and local legislation in relation to the collection, processing, keeping, use and disclosure of personal data.

The ASA Code also has a specific section on online behavioral advertising and the obligations of advertisers to notify users of their data collection and provide an opt-out mechanism for collection of that data.

1.4 How is privacy law enforced in Ireland? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The primary source for enforcement is the Data Protection Commission. Whilst that office (in various guises) had been in place since the original Data Protection Act 1988, following the introduction of the GDPR, a new Data Protection Commission was established. It is the national independent supervisory authority in Ireland, with responsibility for upholding the fundamental right of individuals to have their personal data protected. Its statutory powers, functions and duties derive from the Data Protection Act 2018, the GDPR, the EU Law Enforcement Directive, as well as from the Data Protection Acts 1988 to 2003. The Data Protection Commissioner is appointed by the Government, but is an independent role and exercises its functions independently.

Additionally, individuals who claim to suffer damage as a result of a data breach can bring proceedings for damages through the courts.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Ireland?

See the European Union chapter, as same will apply in Ireland.

2.2 Does privacy law in Ireland apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, Irish privacy law can, where applicable, apply to companies outside of Ireland. The Data Protection Act 2018 will also be relevant if a company, although based outside Ireland, is processing personal data in Ireland.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Ireland?

Personal data is defined in the GDPR (see European Union chapter), and Ireland has adopted that definition.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Generally, this is covered by the GDPR. Further details are contained in the European Union chapter.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter, as same will apply in Ireland.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The obligations as set out in the European Union chapter will apply.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

This is governed by the GDPR which splits the roles between controllers and processors. The European Union chapter contains the relevant information which would also be applicable in Ireland.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, as per the European Union chapter, under the GDPR the processing of personal data requires a lawful basis. The basis is set out in the European Union chapter and Ireland will apply the same criteria.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The obligations as set out in the European Union chapter will apply as the information required is derived from the GDPR.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

The rights as set out in the European Union chapter will apply.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

These are established under the GDPR and ePrivacy Regulations so the position as set out in the European Union chapter will apply.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

This is addressed in the GDPR as implemented in Ireland and the position as set out in the European Union chapter will apply.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

This is addressed in the GDPR as implemented in Ireland and the position as set out in the European Union chapter will apply.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

This is addressed in the GDPR as implemented in Ireland and the position as set out in the European Union chapter will apply.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The principles of the GDPR and the ePrivacy Regulations apply and details are contained in the European Union chapter. Affirmative consent of the recipient is required. Self-regulation would be through the ASA in Ireland implemented through its code on marketing communications. In addition, the Data Protection Commissioner publishes guidance on direct marketing rules.

The Data Protection Act 2018 prohibits direct marketing to, or the micro-targeting of, children. The Act sets the defined age for a child (from a data perspective) as being under 16 years of age.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The principles of the GDPR and the ePrivacy Regulations apply and details are contained in the European Union chapter. Again, the Data Protection Commissioner has published guidance on cookies and other tracking technologies.

7.3 How are loyalty programs and promotions regulated under privacy law?

These are as set out in the European Union chapter on the GDPR.

7.4 How is social media and influencer marketing regulated under privacy law?

These are as set out in the European Union chapter on the GDPR. The ASA in Ireland has specific guidance on social media and influencer marketing but it does not highlight privacy issues.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

These are as set out in the European Union chapter on the GDPR. The ASA in Ireland has a separate chapter in its *Code of Standards for Advertising and Marketing Communications in Ireland* on online behavioral advertising and the rules therein are primarily focused on transparency and notice obligations.

The Data Protection Commissioner in Ireland is particularly focused in this area and in October 2024, it concluded an inquiry into LinkedIn which assessed the lawfulness, fairness and transparency of LinkedIn's processing of its EU/EEA members for the purposes of behavioral analysis and targeted advertising. A fine of €310 million was imposed on LinkedIn, in addition to an order to bring its processing operations into compliance.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

These are as set out in the European Union chapter on the GDPR.

7.7 How is location-based advertising regulated under privacy law?

This is based on the GDPR and the ePrivacy Directive and as set out in the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

These are as set out in the European Union chapter on the GDPR.

7.9 How is advertising to children and minors regulated under privacy law?

This would be governed by the GDPR and the ePrivacy Directive and generally as set out in the European Union chapter. The Data Protection Act 2018 prohibits direct marketing to, or the micro-targeting of, children. The Act sets the defined age for a child (from a data perspective) as being under 16 years of age.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific regulations in Ireland other than the GDPR, and the position would be the same as set out in the EU chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

Targeted advertising has been an area of focus with the Data Protection Commissioner in Ireland. This is not necessarily solely online behavioral advertising, but more the practice of behavioral analysis across multiple different platforms, leading to specific marketing depending on the users' traits, habits, interactions etc. The Data Protection Commissioner has identified transparency and consent as two key issues which are lacking in this practice, and has taken action against offending companies.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes, these are established under the GDPR and set out in the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

None beyond those set out under the GDPR and explained in the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Ireland? Are there minimum standards? Does this differ by sector or size of the entity?

The GDPR as implemented in Ireland through the Data Protection Act 2018 does not detail specific security measures that a data controller or data processor must have in place, though the European Communities (Electronic Communications Networks and Services) (Privacy and Communications) Regulations 2011 detail some requirements specific to the electronic communications services sector.

The Data Protection Commissioner has published detailed guidance on data security on its website.

9.2 How are personal data breaches regulated in Ireland? What are the requirements for notification and response?

The requirements are established under the GDPR and set out in the EU chapter. The supervisory authority in Ireland is the Data Protection Commission and the timeframe for notification is a maximum of 72 hours from the data breach. As with the GDPR, the individual concerned must also be notified. The Data Protection Commission makes a breach notification form available for such notifications.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

There are a number of different claims/sanctions that can arise:

- (a) administrative fines by the Data Protection Commissioner;
- (b) civil claims by another controller or processor;
- (c) criminal charges; and
- (d) civil claims by an individual.

Possible administrative fines are based on the GDPR and are set out in the European Union chapter. If a controller or processor is ordered to pay such a fine due to the mistake of another, they can, in turn, bring a civil claim (see (b) above) against that third party (eg, another processor who they allege is actually liable). The Data Protection Act 2018 also provides for a number of criminal penalties, including fines and/or imprisonment, depending on the offense and whether it is a summary conviction or on indictment. The Data Protection Commission has been working for a number of years now with other European data regulators in relation to companies with a head office in Ireland.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, individual consumers can bring a private action in the courts for damages or other remedies, such as an injunction, arising out of a data breach. These can be brought in the Circuit Court or High Court. Such actions are rare, but the option is certainly there. The remedy would depend on the original breach and the damage caused, and any financial damages would generally be quantified.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The Data Protection Commissioner is one of the more active European enforcement bodies, primarily due to the presence of multinational companies using Ireland as their primary base in Europe,

In May 2025 the Data Protection Commissioner concluded an investigation against TikTok Technology Limited relating to transfers of personal data of users of that social media platform from the European Union to China which resulted in a €530 million fine for breaches of GDPR in relation to transparency.

In December 2024 a Data Protection Commissioner investigation against Meta in relation to data breaches was concluded and resulted in a fine of €251 million.

On a much smaller scale, in December 2024 the Data Protection Commissioner brought a successful prosecution through the District Court in Ireland in relation to a company that failed to properly provide an opt-out mechanism for direct marketing communications and had previously been warned about the issue.

Lastly, there have been private actions taken by consumers against companies for damages arising from a data breach and said consumers have successfully been awarded damages.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Ireland?

No specific cultural considerations relating to privacy in Ireland.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Firstly, following court decisions both in Ireland and in the European Union, it is clear that private actions taken by consumers are increasing, and companies need to be aware of the increased challenge such claims may bring.

Issues relating to data protection and child safety are likely to come to the fore as 2024 saw the implementation of the EU Digital Services Act in Ireland and an Online Safety Code. Age verification is an expected hot topic and we expect to see guidance for data controllers and processors in these areas.

Lastly the EU Artificial Intelligence (‘AI’) Act came into direct operation in 2024, and it is expected that those providing AI systems will face challenges in respect of how that operates with the GDPR and local regulations.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

None, other than as set out in this chapter or highlighted in the European Union chapter.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The primary legislation in Ireland remains the same. The Data Protection Commissioner has become more active in large-scale investigations of offending multinational companies and will work with European counterparts as part of that process. That increased activity seems to have been triggered by initial reviews showing many of the companies investigated were not compliant in areas of transparency and consent, and the data of consumers was being processed without proper consent or transparency.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Much of the landscape is changing with the emergence of AI and automated systems for much of the data processing and collection work. Companies face the challenge of hoping to lower their costs by taking advantage of these systems but at the same time remaining compliant with an increasingly vigilant Data Protection Commissioner and facing the risk of multi-million euro fines for non-compliance.

12.3 What do you envision the privacy landscape will look like in five years?

The AI Act and the emergence of AI will have changed the landscape. We expect the Data Protection Commissioner to extend its authority to privacy issues with AI. There will, perhaps, be a focus on putting proper frameworks in place to use AI and retain proper data protection controls.

From a corporate perspective we expect companies to become increasingly aware of their obligations, and company boards to include data protection in normal governance reviews.

ITALLY

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Italy.

In Italy, privacy is regulated by:

- (a) **Constitutional rights:** Although the Italian Constitution does not contain a specific provision concerning data protection and privacy rights, Italian commentators agree in recognizing a constitutional value to such rights, considered as inviolable human rights of new generation.
- (b) **European law:** From an EU regulation perspective, the main source of law is the EU General Data Protection Regulation ('GDPR').
- (c) **National law:** The first Italian privacy regulation was Law No 675 of December 31, 1996, implementing Directive 95/46/EC, the first example of a complete and systematic discipline on the matter, which considered privacy and data protection as fundamental rights. This law was repealed and replaced by Legislative Decree No 196 of June 30, 2003 ('Data Protection Code') which implemented the EU ePrivacy Directive.

Following the entry into force of GDPR, the Italian legislator issued Legislative Decree No 101 of August 10, 2018, which amended the Data Protection Code in order to adapt the national legislation to the GDPR.

As for interpretation and enforcement, the competent supervisory body is the Garante, which also issues resolutions and guidelines aimed at interpreting the laws.

1.2 What are the primary laws regulating privacy in Italy? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The primary source for data protection in the European Union and, consequently, Italy, is the GDPR.
- (b) However, through the use of opening clauses, the GDPR provides the possibility for the Member States to regulate certain privacy aspects. Some of these opening clauses have been transposed into the Italian legal system by the Data Protection Code; for example:
 - (i) in cases of data processing for the performance of a task carried out in the public interest or in the exercise of official authority, the legal basis for the processing is exclusively a rule of law, regulation (in cases provided for by the law itself), or general administrative acts;
 - (ii) the Garante has been given power to promote the adoption of rules of conduct for the processing of personal data in certain situations, and has approved rules of conduct concerning processing activities carried out for the following purposes:
 - journalistic activities,
 - scientific or statistical research,
 - scientific or statistical research in the context of the National Statistical System,
 - investigations in defense of a claim or defending a right in court, and
 - archiving purposes in the public interest or for historical research.
 - (iii) the Garante is required to set out safeguards applying to the processing of genetic, biometric and health data;

- (iv) principles applying to the processing of data relating to criminal convictions and offences are to be set out by decree of the Italian Ministry of Justice.
- However, to date, items (iii) and (iv) have not yet been carried out (see, further, question 3.2).
- (c) With regard to the legal framework on the protection of personal data in the field of advertising, the following are important:
 - (i) the Data Protection Code (which implemented the EU ePrivacy Directive and adapted the national legislation to the GDPR);
 - (ii) Law No 5 of January 11, 2018 on telemarketing ('Telemarketing Law') which provides for the registration and functioning of the opt-out register and establishment of national prefixes for calls for statistical, promotional and market research purposes;
 - (iii) Presidential Decree No 26 of January 27, 2022 which amends the regulations in force on the registration and operation of the opt-out register for calls for statistical, promotional and market research purposes ('Opt-out Register Decree');
 - (iv) Guidelines on cookies and other tracking tools of June 10, 2021, issued by the Garante ('Cookie Guidelines');
 - (v) Guidelines on marketing and against spam of July 4, 2013, issued by the Garante ('Guidelines on marketing and against spam').

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Italy does not have any self-regulatory body enforcing privacy law, rather, the Garante acts in this capacity (see question 1.4).

1.4 How is privacy law enforced in Italy? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Garante is the authority which enforces privacy law in Italy. The Garante is an independent authority whose main purpose is to protect the fundamental rights and freedoms of data subjects by checking that data processing activities comply with national and European laws.

The Garante carries out several tasks. For instance, it:

- (a) examines complaints lodged pursuant to national and European law;
- (b) reports and refers any facts that can be considered as crimes/felonies prosecutable ex officio; and
- (c) draws up an annual report on the activities it has carried out and the state of implementation of privacy legislation.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Italy?

See the European Union chapter.

2.2 Does privacy law in Italy apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

See the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Italy?

See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

Italy has made further provisions in the Data Protection Code:

- (a) with regard to the processing of personal data concerning children, the Data Protection Code establishes that a child who is at least 14 years old (rather than 16, which is the age set by the GDPR) may consent to data processing in relation to an offer of information society services;
- (b) with regard to the processing of genetic, biometric and health data, the Data Protection Code establishes that the Garante will adopt a specific resolution detailing further safety measures; and
- (c) with regard to the processing of data concerning criminal convictions and offences, the Data Protection Code provides that the Italian Ministry of Justice will adopt a decree identifying adequate guarantees for data subjects' rights and freedoms to be adopted in processing such data.

However, the required resolution and decree (see (b) and (c) above) have not yet been adopted, and so, during this transitional period, the Garante has issued a resolution in order to identify which provisions contained in five general authorizations (applicable under former legislation) are still effective, as being compatible with the GDPR and the Data Protection Code. These five general authorizations concern the processing of the following categories of personal data:

- processing of special categories of personal data in the employment relationship;
- processing of special categories of personal data carried out by associative bodies, foundations, churches and religious associations/communities;
- processing of special categories of personal data by private investigators;
- processing of genetic data; and
- processing of personal data carried out for scientific research purposes.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

In addition, companies should provide information relating to the means used to send marketing communications—ie, automated phone calls and similar arrangements (faxes, emails, SMS and MMS) and/or traditional mechanisms (mail and operator-assisted calls). Moreover, under the Telemarketing Law, in the event of transfer of data relating to telephone numbers to third parties for marketing purposes, the data controller is required to inform the data subjects of the identity of the person to whom the data are transferred.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

Consumers have also the right to file a complaint before the Garante if they deem that the processing of their personal data is unlawful.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the GDPR, the Data Protection Code, the Guidelines on marketing and against spam and the Telemarketing Law, companies must obtain consent or provide opt-out mechanisms for advertising activities depending on the nature of the data processing involved as follows:

(a) Consent

- (i) Explicit, informed, and freely given consent is required before processing personal data for targeted advertising, tracking, using cookies and similar technologies. Consent must be obtained through a clear affirmative action and can be withdrawn at any time.
- (ii) According to the Data Protection Code, consent (ie, an opt-in mechanism) is required for email, SMS, MMS or other kind of messages, telefax, and automated calls aimed at marketing, marketing research, the sending of commercial communications or the proposing of direct sales.
- (iii) If a user who has previously given consent to automated phone calls wishes to revoke their consent, they can register in the opt-out register, according to the Telemarketing Law.
- (iv) If the call is conducted by a physical operator, marketing calls are permitted without the recipient's prior consent, provided that the number has not been registered by the recipient in the opt-out register (opt-out requirement).

- (v) While the Garante deems consent provided for automated marketing to include consent to marketing by traditional means, it also provides that data subjects must be able to revoke their consent in relation to each method.
 - (vi) In addition, the Garante requires that generic and broad formulae are not used to collect data subjects' consent for marketing communications (eg, a unique consent is required for the sharing of personal data with each of several non-identified third parties and for each of several marketing channels).
 - (vii) When marketing communications are sent simultaneously to mailing lists, the addresses contained in the mailing list must be obscured to other recipients (eg, through a blind carbon copy).
 - (viii) The Garante also requires specific measures to demonstrate the moment when the data controller obtained consent by users.
- (b) **Legitimate interest and opt-out:** Companies may rely on legitimate interest for certain advertising activities, such as contextual advertising or direct marketing via postal mail. Additionally, the Data Protection Code provides for the so-called 'soft-spam exception' applying only to email marketing communications. Accordingly, data controllers may rely on legitimate interest if the following conditions are met:
- (i) the data controller uses the email address provided by the data subject in the course of a previous sale of a product or service;
 - (ii) the product or service advertised is similar to the one previously sold; and
 - (iii) the data subject has been duly informed as to the purposes and mechanisms of the processing and is given a simple opportunity to refuse or opt out of receiving marketing communications (each communication must include an opt-out mechanism)
- (c) **Behavioral advertising and tracking technologies:** The use of cookies, pixels, and similar tracking tools requires prior consent unless they are strictly necessary for website functionality.

It is important to highlight that the Garante requires data controllers to obtain two separate consents for marketing purposes and for profiling as, according to the Garante, profiling constitutes a purpose of the processing (rather than a modality) and, therefore, a separate legal basis for the processing is required.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for privacy law obligations.

In addition, in the Italian framework, marketing communications are regulated by:

- (a) the Data Protection Code;
- (b) the Guidelines on marketing and against spam; and
- (c) the Telemarketing Law.

Under the Data Protection Code, data processing for promotional purposes may be performed by way of automated or similar tools (eg, emails, faxes, SMS, or MMS) only if the data controller obtains the recipient's prior consent (opt-in requirement) (see question 5.3). Moreover, the Garante has specified that it is forbidden to send marketing communications by such means without the recipients' prior consent, even if the personal data has been taken from publicly available sources, websites or documents.

Data controllers should inform recipients clearly and appropriately by means of a proper notice containing all the elements listed in the GDPR and, in addition, information relating to the means used to send marketing communications, ie, automated phone calls and similar arrangements (faxes, emails, SMS and MMS) and/or traditional mechanisms (mail and operator-assisted calls), as stated in question 5.1. Notably, communications requiring users to provide consent for marketing purposes are considered as marketing communications by the Garante.

Please refer to our answers to question 5.3 with regard to the other measures to be implemented in case of marketing communications.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

In addition, in accordance with the Data Protection Code and the Cookie Guidelines, cookies are regulated differently according to the purposes for which they are intended to be used.

According to the Cookie Guidelines, cookies may be distinguished into two major groups: technical cookies (including browsing or session and functional cookies) and profiling cookies:

- (a) **Profiling cookies:** the manager of the website visited by the user ('Publisher') must:
 - (i) provide a simplified notice, consisting of an initial 'short' notice in an overlay banner on the home page, which is supplemented by an 'extended' notice to be accessed via a clickable hyperlink; and
 - (ii) obtain the user's consent to use profiling cookies. In particular, the consent request to the use of cookies must be included in the banner displaying the short information notice and, after the user has made their choice, it must not be presented again until six months have passed, unless specific circumstances are met. Consent must be expressed by clear affirmative action; thus, the mere scroll down of the webpage does

not constitute a valid way of collecting consent. Furthermore, so-called ‘cookie walls’ contradict the principle of freedom of consent and are deemed unlawful.

The Cookie Guidelines provides specific requirements as to the characteristics of the banner, which must also include:

- an ‘X’ in the upper right corner that can be used to close it (in which case, only technical cookies may be installed);
- a warning to the effect that if the banner is closed (eg, by clicking on the ‘X’ in the top right corner) the default settings are left unchanged and therefore browsing can continue without cookies or other tracking tools other than technical ones;
- a control for the user to accept placement of all cookies; and
- a link to an additional dedicated area where the user can select, individually, the functionalities, the third parties, and the cookies that the user consents to install.

Users must be able to easily change their choices at any time, therefore, the Publisher must place a hyperlink to the dedicated area for the management of cookie choices in the footer of the website, whose functionality is made explicit by stating ‘review your cookie choices’ or similar.

The Publisher is the data controller in respect of the cookies installed directly by its own websites.

As to cookies placed by other websites or web servers (‘Third Parties Cookies’), the Publisher cannot be considered a joint controller with these third parties, but only as a sort of technical intermediary between them and users. As such, the Publisher must provide users with a link to the third party’s website and its notice and consent wording. In order to do this, Publishers are required to obtain links to the webpages containing the information and consent forms relating to Third Parties Cookies when entering into the relating agreements.

- (b) **Technical cookies**, on the other hand, do not require prior informed consent. Publishers must provide notice in the way they deem most appropriate.

Analytic cookies are assimilated to technical ones exclusively when:

- (i) they are used for the sole purpose of producing aggregated statistics concerning a single website or mobile app;
- (ii) if provided by third parties, suitable tools are adopted to reduce the identification power of cookies (eg, by masking significant portions of IP address) and the third parties undertake not to combine the data obtained from these cookies with other information already available to them.

The Garante has also launched a public consultation to assess the lawfulness of processing activities conducted through the so-called ‘pay or ok’ models (also known as ‘pay or consent’ or ‘consent paywall’ models), used especially by online editors and newspapers. ‘Pay or ok’ models require users to choose between paying for a subscription or consent to the processing of their personal data for commercial profiling purposes, through cookies and tracking tools, to access content, services, or features offered online.

7.3 How are loyalty programs and promotions regulated under privacy law?

The Garante has stated that a data subject’s consent is not required in the context of loyalty programs, to the extent that the personal data are processed only for the purpose to execute the program.

Conversely, a data subject’s specific and informed consent is required for any other purpose (including marketing and profiling).

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

In addition, the Guidelines on marketing and against spam provide clarifications on the following specific cases that may occur specifically to social network users:

- (a) Users receive a marketing message from a company that has obtained their personal data from their public profile on a social network: In this case, the data processing is unlawful unless the sender can show proof of the recipients' prior, specific and free consent under the Data Protection Code.
- (b) The user is a 'fan' of a given company or has joined a group of followers of a given brand, personality, product or service and then receives marketing messages related to such brand, product, service or company: This data processing is lawful if it is clear and unequivocal that the recipients, by their behavior, also intended to express consent to receiving marketing messages from that company. On the other hand, if the recipient unsubscribes from the abovementioned group or stops following the brand, product, service or company or objects to further marketing messages, any marketing message sent thereafter will be considered unlawful.
- (c) Marketing messages are sent to a user's contacts (so-called 'friends') by companies by using the phone numbers or email addresses accessible within the social network: In this case, the marketing messages are sent lawfully only if a prior specific consent has been obtained.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising is based on user profiling mechanisms.

According to the Guidelines on marketing and against spam, in the case of personal data processing for profiling purposes, data subject must be provided with adequate, clear and complete information, specifying, eg, the purpose of such profiling and which mechanisms are expected to be used in data processing.

Moreover, so-called 'targeted spam', based on profiles of social network users, may increase, since the providers of such social network platforms tend to merge profiles from different services on a given platform in order to raise detailed information on users. Thus, they may receive messages customized to their interests and preferences. With regard to so-called 'social spam', refer to question 7.4.

Finally, concerning profiling cookies, please refer to question 7.3.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter. Besides, it is important to note that location-based advertising can also be considered as a form of profiling.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter. The Garante also requires companies to adopt age verification systems in the provision of their services online to the requirements of the Data Protection Code.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific rules on the use of artificial intelligence for advertising purposes. The general rules on advertising and profiling apply.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

In addition, under the Data Protection Code, unlawful data transfer damaging the data subject, made for purposes of gaining a profit or causing harm to a third party, is a crime punishable with imprisonment ranging from one to three years.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Italy? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

Additionally, further security requirements may apply according to the cybersecurity framework under the Italian law. For instance, Legislative Decree No 138 of 2024 implemented the NIS2 Directive, establishing specific cybersecurity requirements for in-scope entities.

9.2 How are personal data breaches regulated in Italy? What are the requirements for notification and response?

See the European Union chapter.

Moreover, as of July 1, 2021, notification of a personal data breach must be sent to the Garante through a specific digital procedure, made available on the Garante's website.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

In addition, the Data Protection Code provides that personal data, processed in violation of the relevant provisions of the law, may not be used unless the Garante has indicated to the data controller or data processor the necessary amendments and additions to the processing activities and has verified their implementation.

Moreover, the following violations of the Data Protection Code can lead to criminal penalties:

- (a) Unlawful data processing for purposes of gaining a profit or damaging to data subjects, in case of processing of traffic data, location data or spam communications, to the extent that the data subject suffered a damage (up to 18 months' imprisonment);
- (b) Unlawful processing of special categories of personal data and personal data relating to criminal convictions and offences for purposes of gaining a profit or damaging data subjects (up to three years' imprisonment);
- (c) Unlawful data disclosure and diffusion of an automated archive or a substantial part of it containing personal data being processed on a large scale for purposes of gaining a profit or harming third parties and damaging data subjects (up to six years' imprisonment);
- (d) Fraudulent acquisition of personal data in relation to large-scale data processing (up to four years imprisonment);
- (e) Untrue declarations submitted to the Garante (up to three years' imprisonment)
- (f) Intentional interruption or disturbance of the regular proceeding before the Garante or the investigations carried out by the Garante (up to one year's imprisonment).;
- (g) Failure to comply with provisions issued by the Garante (up to two years' imprisonment);
- (h) Failure to comply with other mandatory obligations relating to personal data protection of employees (criminal fine of up to €1,549 or up to one year's imprisonment (or, in severe cases, both); and
- (i) Unlawful transfer of personal data, for the purpose of gaining a profit or damaging to data subjects (up to three years' imprisonment).

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Under the Italian legal framework, the Garante is very active in the enforcement of privacy laws regulating marketing and profiling. Between 2023 and 2025, the Garante has issued several significant decisions addressing unlawful data processing for marketing and profiling purposes:

- (a) The Garante fined Energia Pulita Srl €300,000 for having used generic formulas to collect data subjects' consent (eg, data subjects were not able to give specific and separate consent for the means used for sending marketing communication), as well as for not having adequately monitored third parties involved in promotional phone calls.
- (b) This decision follows the Garante's approach where it fined Sky Italia €842,062 for not having obtained a new, specific and explicit consent to communicate personal data to third parties

for marketing purposes, as well as for having relied upon legitimate interest as the legal basis for sending promotional communications to data subjects through phone and SMS, in breach of the Data Protection Code.

- (c) Moreover, in several decisions the Garante has fined companies for not having implemented adequate measures to demonstrate the moment when the controller obtained data subjects' consent for marketing purposes.
- (d) Notably, the Garante has fined Ediscom SpA €300,000 for having illegally enticed data subjects to consent to the processing of their personal data for marketing purposes through the use of dark patterns.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Italy?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Considering the Garante's case law and the evolving regulatory framework at the EU level, it is possible to state that the Garante has been focusing especially on artificial intelligence and the protection of minors online as well as on marketing and profiling during its enforcement activities.

Indeed, it is possible to highlight the following hot topics:

- (a) **Impact of digitalization:** The Garante has focused on providers of artificial intelligence systems who train their models using users' data and do not employ any measure for the protection of children online.

On April 29, 2025, the Garante published a press release informing citizens that Meta will process data from public posts of users over the age of 18—including posts, comments, captions, photos, and data generated through the use of its AI services (such as information entered into its conversational agent on WhatsApp, Facebook or Instagram)—to train and improve its Meta AI chatbot or its language models like LLaMA. The Garante encouraged individuals to understand the potential consequences and implications of the use of their personal data for training artificial intelligence models, and to exercise their rights (eg, the right to object) accordingly, with full awareness.

Meanwhile, the Garante has begun an investigation alongside other European data protection authorities to assess whether Meta's proposed data processing activities, based on legitimate interest, comply with data protection regulations.

The Garante continues to give particular attention to the lawfulness of these practices, the real effectiveness of the right to object, and the compatibility between the original purposes of data processing and this new method of using data.

In this regard, it is important to mention that the Garante's enforcement and investigation activities on artificial intelligence systems have been very frequent during the last years. For example:

- (i) The Garante has imposed a €5 million fine on Luka Inc, for the processing of personal data related to its chatbot Replika. Replika is a AI-powered chatbot, which uses a written and voice interface, to 'generate' a 'virtual friend' for users that can in this way have a virtual confidant, therapist, romantic partner, or mentor. The Garante had

imposed a provisional limitation on the data processing activities carried out by Luka Inc in 2023, and then started an investigation for the alleged violation of several data protection rules. In the end, the Garante found that Luka had implemented an inadequate age verification system, lacking the technical and organizational measures necessary to enhance the protection of children.

During the investigation, the Garante had required Luka to provide clarifications on certain aspects (eg, on the measures adopted to protect personal data during the development and training of the large language model behind Replika); the decision states that these elements will be subject to a further specific investigation.

- (ii) Moreover, the Garante has fined OpenAI €15 million and ordered it to carry out a six-month information campaign on data processing related to ChatGPT. The Garante found ChatGPT in violation of the privacy by default and privacy by design principles, as it did not provide for any age verification measure to prevent access to the service to data subjects under the age of 13 and did not ensure the involvement of the holder of parental responsibility in the registration process of minors between the age of 13 and 14. Nonetheless, the Garante's resolution has been suspended by the Court of Rome.
- (iii) On May 20, 2024, the Garante issued guidance on how to protect personal data published online from web scraping, ie, from the indiscriminate collection of personal data on the internet for the purpose of training generative artificial Intelligence models. In this guidance, the Garante suggested some technical measures that entities can adopt to prevent or, at least, hinder web scraping (for example, the inclusion of anti-scraping clauses in their terms of service; the creation of reserved areas, accessible upon registration; the monitoring of traffic to web pages; etc).
- (iv) The Garante blocked data processing activities carried out by Hangzhou DeepSeek Artificial Intelligence and Beijing DeepSeek Artificial Intelligence on Italian users' data for the provision of their DeepSeek service. The Garante also opened an investigation in this regard.

(b) **Internet and electronic communications services:** The Garante has given particular focus to:

- (i) how consent is collected and appropriate information is provided;
- (ii) the failure or delay in responding to data subjects' access requests to traffic data for judicial purposes;
- (iii) the excessive data retention period of traffic data; and
- (iv) the use of publicly accessible databases for sending unsolicited promotional messages.

Moreover, the Garante has taken actions against platforms that do not ensure compliance with the rules applying to the processing of children personal data, including the implementation of proper age verification systems.

(c) **Marketing and profiling:** As stated in question 10.3, the Garante has sanctioned a company for using dark patterns in its marketing communications and adopted several decisions regarding unlawful telemarketing (eg, the decision regarding Energia Pulita Srl and the so-called 'consenso omnibus').

Finally, as mentioned above, the Garante has recently launched a public consultation to assess the lawfulness of profiling processing activities conducted through the so-called '**pay or ok**' models.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Garante is very active in enforcing data protection laws, in particular with respect to the hot topics (see question 11.2).

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

During the last years, the development of new technologies, such as artificial intelligence, has posed new challenges and risks, including risks related to the protection of personal data. In this context, the European Union adopted several acts regulating the evolving digital landscape, with a strong emphasis on privacy, cybersecurity and data governance. For instance, the AI Act, the Data Act, and the NIS2 Directive.

In addition, as to the local level, Italy is currently discussing its own AI law, aimed at introducing specific rules in addition to those laid down under the EU AI Act, and this might impact Italian data protection legislation.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

As the European Union accelerates its digital transformation agenda, one of the most relevant challenges for companies is the rising complexity of EU legislation. Companies are required to comply with a very layered framework of overlapping obligations, thereby having to coordinate the efforts of their legal and IT departments to stay aligned with the law.

This fragmentation demands a constant monitoring of legislative developments, and the increasing number of obligations requires companies to reshape their governance frameworks, as well as to invest in cybersecurity measures and AI risk management systems to comply with the law. Although the regulations generally include exceptions applying to small and medium-sized enterprises, they may struggle to implement such sophisticated safeguards.

Companies should attempt to adopt a holistic and forward-looking approach by trying to develop and improve their business activities in compliance with these emerging obligations. This will help them to remain competitive in the digital economy.

12.3 What do you envision the privacy landscape will look like in five years?

In the next five years, the privacy landscape is likely to become more complex and layered. We can expect the European Union to continue pursuing its digital transformation strategy, attempting to always keep up with innovative technologies, especially artificial intelligence.

At the same time, there is a clear interest at the EU level in enhancing the productivity and competitiveness of European companies, especially with respect to their competitors in China and the USA. The European Union aims to place innovation at the heart of European renewal, while removing other constraints holding back growth.

As highlighted in Mario Draghi's report on the Competitiveness Compass, 'Europe must be the place where tomorrow's technologies, services, and clean products are invented, manufactured and marketed, as we stay the course to climate neutrality'.

This dual ambition will certainly create a challenge. On one hand, the European Union remains deeply committed to its core regulatory values. On the other hand, there is an interest in simplifying the regulatory framework to ensure EU companies' further growth. For instance, the European Commission published a proposal of regulation including a simplification of the book-recording obligations under the GDPR.

The European Union's main challenge over the next years will thus be finding a fair balance between the aim of supporting innovation, on one hand, and the need to ensure the fulfillment of the EU regulatory framework.

We believe that, in this context, the boundaries between the different legal sectors such as copyright, data protection or cybersecurity will blur, and the regulatory framework will become even more comprehensive and interconnected.

It will be fascinating to observe how this legal framework will continue to evolve.

 LATVIA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Latvia.

In Latvia, privacy is regulated both on the domestic and on the EU level. On the domestic level, the right to private life is fixed in the Latvian Constitution. In addition, data protection is partly regulated by several laws, such as the Personal Data Processing Law and the Law on Information Society Services.

On the EU level, the most important law is the EU General Data Protection Regulation ('GDPR'). Privacy-related rights are also included in the Charter of Fundamental Rights of the European Union as well as other legislation, such as the ePrivacy Directive. As a general rule, the legal acts of the European Union are binding in Latvia.

See also the European Union chapter.

1.2 What are the primary laws regulating privacy in Latvia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) Firstly, the GDPR is directly applicable. It is the key privacy regulating law as it regulates all aspects of the processing of personal data.
- (b) Secondly, privacy matters are also regulated by the Latvian Personal Data Processing Law, which provides for rules regarding the local data protection authority, data protection officers and their competence, as well as for certain exceptions on data protection rights and processing activities in accordance with the GDPR. Similarly, the Latvian Law on Information Society Services implements the provisions of the ePrivacy Directive.
- (c) There are other sector-specific laws (eg, on the rights of patients, using DNA data, using personal data in the context of criminal and administrative processes and other acts) that touch upon privacy within a specific context.
- (d) Finally, there are guidelines of the Data Protection Authority and sector-specific organizations (such as in the area of employment, electronic communications, banking and anti-money laundering).

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation in privacy practices is rare at the domestic level and plays a minimal role in complementing statutory requirements for advertising. For further details, see the European Union chapter.

1.4 How is privacy law enforced in Latvia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Latvia has a data protection authority ('Data State Inspectorate') established in accordance with the GDPR and the Latvian Personal Data Processing Law.

Privacy cases can also be submitted for review by a court (both in administrative and criminal cases as well as for claiming losses). The Constitutional Court of the Republic of Latvia also examines some privacy-related cases that concern compliance of laws with the right to privacy set forth in the Latvian Constitution.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Latvia?

Companies that may be subject to privacy law in Latvia are companies that:

- (a) are located in Latvia;
- (b) offer goods or services in Latvia; or
- (c) monitor the behavior of data subjects within Latvia.

The only exemptions are those explicitly mentioned in the GDPR; namely, the processing of personal data in the course of an activity which falls outside the scope of EU law, or the processing of personal data by a natural person in the course of a purely personal or household activity.

2.2 Does privacy law in Latvia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Privacy law applies to companies located outside Latvia pursuant to the GDPR. To that extent please see the answer to question 2.1.

Non-EU controllers or processors must appoint a representative in the European Union who will act as a point of contact for supervisory authorities and data subjects. The representative must be established in one of the Member States where the data subjects concerned are located.

See also the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Latvia?

The definition of 'personal data' in Latvia follows the provisions of the GDPR. See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The applicable legislation in this regard is the GDPR. See the European Union chapter.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

In Latvia, companies are subject to core GDPR obligations, including transparency, data security, impact assessments, and data subject rights management. For further details, see the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The roles are assigned pursuant to the GDPR. See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

In Latvia, companies must establish a lawful basis for processing personal data, such as consent or legitimate interest, in accordance with the GDPR. For further details, see the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Companies must provide clear and comprehensive privacy notices when processing personal data for advertising purposes, including details on the controller, purpose, legal basis, data recipients, data subject rights, and any international transfers, in compliance with GDPR. For further details, see the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

In Latvia, companies must obtain valid consent or provide opt-out mechanisms for advertising activities depending on the legal basis and the communication method used, in accordance with GDPR and the ePrivacy Directive. For further details, see the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Organizations operating in Latvia are expected to implement due diligence measures such as vendor assessments, lawful basis reviews, and DPIAs for advertising activities that present elevated privacy risks. For further details, see the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When engaging in personal data exchanges with third parties, entities in Latvia must establish proper contractual safeguards, including DPAs and international transfer mechanisms, to comply with the personal data protection standards under the GDPR. For further details, see the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Businesses in Latvia working with advertising vendors or partners must ensure GDPR compliance through robust contracts, clear consent protocols, and appropriate data protection measures. For further details, see the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Latvia has country-specific rules on legal bases for marketing activities. For instance, the Latvian Information Society Services Law states that:

- (a) cookies can only be used based on consent (with some exceptions based on the EU-wide guidelines). The requirements for cookies policies and banners are similar to the EU requirements;
- (b) marketing calls and sending phone messages can be performed only based on consent; and
- (c) marketing emails can be sent without consent to existing customers, in relation to goods similar to those already acquired, and where there is an opportunity to object to such marketing activities before personal data is used for this purpose. In all other cases, consent is required. Although recently, in cases of doubt, the Data State Inspectorate has required organizations to rely on consent. Finally, each email must give an opportunity to unsubscribe from such communications.

Postal marketing is clearly regulated. Thus, it is for the controller to decide whether it is possible to rely on the basis of legitimate interest or consent in specific circumstances.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Please see the answer to question 7.1. Although the Latvian Information Society Services Law and relevant guidelines of the Data State Inspectorate refer only to cookies, in practice, the same rules are considered also to be applicable to other tracking technologies.

7.3 How are loyalty programs and promotions regulated under privacy law?

In Latvia, loyalty programs and promotions involving personal data must be based on a valid legal basis and comply with GDPR transparency, data minimization, and consent requirements. For further details, see the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

In Latvia, social media and influencer marketing must comply with GDPR principles regarding legal basis, transparency, consent, and data subject rights. For further details, see the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

In Latvia, targeted advertising requires a valid legal basis such as consent, while contextual advertising generally does not involve personal data and is subject to less strict obligations. For further details, see the European Union chapter.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

In Latvia, digital identity resolution and clean room technologies must adhere to GDPR requirements concerning the identification of a legal basis, transparency, anonymization, and other data sharing safeguards. For further details, see the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

In Latvia, location-based advertising is subject to GDPR rules regarding consent, transparency of processing, principle of data minimization, and special protections for children. For further details, see the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

In Latvia, data brokers must comply with GDPR obligations by ensuring a lawful basis for processing, complying with the transparency and data accuracy principles, as well as upholding other data subject rights. For further details, see the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

In Latvia, advertising to children is strictly regulated under the GDPR, requiring parental consent, heightened transparency obligations, and restrictions on profiling. For further details, see the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

In Latvia, profiling and the use of AI or automated decision-making in advertising are subject to the general GDPR requirements. For further details, see the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

In Latvia, any other specific advertising practices must comply with the general GDPR framework. For further details, see the European Union chapter.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The GDPR rules apply.

There are certain sector-specific limitations and localization requirements. For example:

- (a) human DNA data can be transferred outside of Latvia subject to specific procedures; and
- (b) paper-based accounting data must be stored in Latvia (although digital data can be stored in the EU).

See also the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The same GDPR requirements for cross-border data transfers, including safeguards and transfer mechanisms, apply to discovery or similar proceedings. For further details, see the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Latvia? Are there minimum standards? Does this differ by sector or size of the entity?

Personal data security is regulated by the GDPR.

In addition, some of the local information security requirements are also applicable to personal data. For instance, the National Cybersecurity Law, which transposes the EU NIS2 Directive, sets out security rules for the public sector, entities providing critical infrastructure, and essential service providers.

In addition, the rules of the local financial regulator, the Bank of Latvia, on information technologies and management of security risks provide detailed information security rules for the financial and related sectors.

See also the European Union chapter.

9.2 How are personal data breaches regulated in Latvia? What are the requirements for notification and response?

The GDPR rules apply to cases where there is a pure personal data breach. In cases where data breaches are also information security breaches, additional requirements of the National Cybersecurity Law apply (see question 9.1). If the National Cybersecurity Law applies, the companies concerned must immediately inform the local CERT about an information security incident and cooperate with the CERT while responding to the breach.

Additional specific information security breach notification rules apply to payment services providers under the Law on Payment Services and Electronic Money, as well as the rules of the Bank of Latvia.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The GDPR rules apply. However, there are certain limitations for public sector employees: the monetary penalty is limited to €1,000.

In addition, the Latvian Criminal Law states that criminal sanctions (including imprisonment up to 5 years) may also apply in the following cases:

- (a) illegal activities involving the personal data of a natural person, if substantial harm has been caused;
- (b) illegal activities involving the personal data of a natural person, if performed by a personal data processing controller or processor for the purpose of vengeance, acquisition of property, or blackmail; or
- (c) influencing a personal data processing controller or processor or the data subject, using violence or threats or abusing trust in bad faith, or using deceit in order to perform illegal activities involving the personal data of a natural person.

10.2 Do consumers have a private right of action? What remedies are available to them?

In Latvia, consumers have a private right of action under the GDPR and may seek remedies such as lodging complaints, judicial review, compensation, and collective actions. For further details, see the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In Latvia, enforcement of privacy-related matters is active at the national level, with the Data State Inspectorate aiming to follow up on any potential issues. Notably, the imposed fines are typically reduced if the entity cooperates with the authority and willingly rectifies the breach.

For example, in its decision of 11 November 2024, the Data State Inspectorate ordered a company to revise the cookies on its website to ensure compliance with consent requirements for advertising cookies.

For details on the EU level, see the European Union chapter.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Latvia?

Each year, the Data State Inspectorate tends to pay attention to certain compliance requirements and perform thematic audits (for example, video surveillance or cookies).

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

The Data State Inspectorate takes part in the large-scale regional actions taken by the European Union and the European Data Protection Board. On the national level, however, considerable attention recently has been paid to video monitoring, photography and activities which fall under the exemption of household activities. Recently, the Data State Inspectorate undertook a review of privacy policy compatibility with the GDPR in 30 Latvian-registered companies whose main activity is related to retail sales by mail order or online.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, the privacy landscape has evolved due to increased enforcement of data protection laws like the GDPR and the introduction of revised cybersecurity legislation, and the European Digital Single Market, which carried the adoption of such legal acts as the EU Digital Markets Act and the AI Act. More recently, the EU Data Act (Regulation 2023/2854), Data Governance Act (Regulation 2022/868), and Regulation 2025/327 on the European Health Data Space have entered into force.

The transfer of personal data to the US has also undergone changes, with the invalidation of the Privacy Shield and the introduction of the EU-US Data Privacy Framework.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The primary challenges lie in maintaining ongoing compliance with privacy requirements, which includes regularly updating documentation, complying with the retention periods of personal data and reviewing how the privacy-by-design principle is being implemented. Heightened enforcement risks are also present.

12.3 What do you envision the privacy landscape will look like in five years?

In the coming five years, the privacy landscape is expected to evolve, strengthening the core principles and values enshrined in the GDPR and the European Union as a whole. While no major shifts are expected, the rise of new technologies and AI is bound to receive a regulatory response, with privacy-centric tech becoming the default expectation, especially in the European Union, and particularly in more sensitive sectors such as health or insurance.

LITHUANIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Lithuania.

Privacy is regulated on two levels: that of the European Union and that of the Republic of Lithuania:

- (a) **EU**
 - (i) On the level of the European Union, the most important applicable source of law is the EU General Data Protection Regulation ('GDPR') which came into force in May 2018. It covers all aspects of privacy law insofar as the processing of personal data is concerned.
 - (ii) The protection of personal data is also enshrined in the Charter of Fundamental Rights of the European Union, by which all the institutions, bodies, offices and agencies of the European Union are bound, as are the Member States, which have to comply with it when implementing EU law. All the European Union's actions must therefore be measured against the Charter, in particular EU legislation (Regulations and Directives) and EU administration.
 - (iii) There is also the ePrivacy Directive, which is not directly applicable, but obliges the Member States to implement its regulations into national law.
- (b) **Lithuania**

On a local level there are a few laws addressing the retention terms, processing of a national identification number (personal code), direct marketing, general requirements for advertisements, etc.

1.2 What are the primary laws regulating privacy in Lithuania? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) In Lithuania there are two main acts regulating privacy: the GDPR and the local Law on Legal Protection of Personal Data ('Local Privacy Law').
- (b) In addition, the director of the Lithuanian supervisory authority, the State Data Protection Inspectorate, has issued an Order on Data Processing Operations which Require a Prior Privacy Impact Assessment ('Order on PIA').
- (c) Data retention terms are regulated by the Order of the Chief Archivist on the Index of the General Document and Data Retention Terms (the 'Index').
- (d) Some aspects of advertising are covered by the Law on Electronic Communications, the Law on Unfair Commercial Practice towards the Consumers, and the Law on Advertising.
- (e) Data processing in the mass media is regulated by the Law on Public Information.
- (f) The Civil Code of the Republic of Lithuania briefly covers the main aspects of the use of a person's image.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation doesn't play a big role, because the traditions of self-regulation are not strong in Lithuania. LIMA—the Lithuanian marketing association—is active in four major cities and has an Ethics Code. However, in practice, this Code does not have a substantial impact on the market.

1.4 How is privacy law enforced in Lithuania? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The State Data Protection Inspectorate (<https://vdai.lrv.lt/>) is the main privacy supervisory body.

The State Consumer Rights Protection Authority (<https://www.vvtat.lt/en>) addresses privacy issues related to unfair marketing practices (including that of direct marketing).

The Office of the Inspector of Journalist Ethics (<https://www.zeit.lt/en>) regulates the use of personal data in a mass media context.

There are no self-regulatory bodies in respect of privacy rights in Lithuania.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Lithuania?

According to the Local Privacy Law, legal entities (controllers or processors) which are:

- (a) established in Lithuania;
 - (b) are subject to Lithuanian law due to international public law (eg, embassies and consulates); or
 - (c) whose representative, appointed pursuant to the GDPR, is established in Lithuania,
- are subject to the Local Privacy Law.

2.2 Does privacy law in Lithuania apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the Local Privacy Law applies to:

- (a) legal entities which are subject to Lithuanian law due to international public law; and
- (b) companies' representatives appointed according to the GDPR.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Lithuania?

The Local Privacy Law does not provide a local definition of 'personal data'; thus, the GDPR definition applies.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Local Privacy Law does not provide for an alternative definition of 'sensitive' or 'special' categories of data; thus, data listed in the GDPR is considered sensitive personal data.

However, the Local Privacy Law regulates the personal code—a national identification number provided to a person at birth and carried with them throughout their lifetime. This personal code is used as an identifier in most of the state registries throughout a person's life; therefore, special legal protection of this data element is ensured, whereby a person's personal code cannot:

- (a) be disclosed publicly by any controller/processor; or
- (b) be used for the purposes of direct marketing.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

There is no local regulation in this regard.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Key privacy-related obligations for the advertising business are as follows:

- (a) Legal collection of data (advertising, especially direct marketing, usually needs the consent of the user, which is rather difficult to obtain, and must meet all the GDPR standards for consent);
- (b) Transparency (posting of the privacy policy);
- (c) For companies involved in provision of real-time bidding advertisements, it is important to follow the rules on targeting cookies (see questions 7.1 and 7.2);
- (d) Advertisements which involve children's data require companies to conduct a privacy impact assessment (based on the Order on PIA);
- (e) An 'unsubscribe' option must be included in all direct marketing communication;
- (f) It is important to keep data processing records and appoint a data protection officer ('DPO'), if the data is processed constantly on a large level;
- (g) Keep processor records if the advertising company acts as a processor (eg, provides a newsletter sending platform); and
- (h) Sign a data processing agreement, if the advertising company acts as a processor.

Please note that there is no obligation to register with the local supervisory authority.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The GDPR assigns roles to companies based on how they process data:

- (a) **Controllers** are the companies which, in their own capacity, or together with others, define processing purposes or are obliged by law to process data.
- (b) **Processors** are usually the entities which provide technical or other types of assistance in processing data, and act solely on the instructions of a controller.

The Local Privacy Law does not provide any additional rules in this regard.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, always. This is a mandatory requirement stemming from the GDPR; thus, all data collection and usage for the purposes of marketing must have an opt-in consent (there is an exception only for email marketing for current clients—in this case, opt-out consent is necessary (please see question 5.3)).

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Consent for advertising activities is a mandatory requirement and is always required. As a rule, an active prior consent (opt-in) is required for any type of direct advertising.

One exception applies—pursuant to the Law on Electronic Communications, email can be used for direct marketing on these conditions:

- (a) the email address was collected from an existing client;
- (b) the marketing offer is for similar goods or services to those previously supplied;
- (c) the marketing offers goods or services of the sender's own store, not those of its partners/other group entities, etc;
- (d) there is an 'unsubscribe' button each time an email is sent; and
- (e) when the email was collected a client was offered the possibility to reject marketing.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Local laws do not specifically regulate such contractual relationships. General provisions for contract conclusion/termination/interpretation of the Civil Code apply.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

This is not regulated. We advise including:

- (a) a description of data categories that are received pursuant to the contract;
- (b) allowed processing purposes; and
- (c) a prohibition on reselling data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Compliance with GDPR principles (most importantly legitimacy, minimization and data security).

Additionally, pursuant to local legal requirements, a privacy impact assessment must be carried out if children's data is to be used for marketing.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Lithuania does not have separate regulation for targeted advertisement. The provisions of the Law on Electronic Communications apply because, in essence, targeted advertising is closely related to the use of advertising cookies/technologies. Since advertising/targeting cookies are deemed non-essential, they require the prior opt-in consent of the end user.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of cookies and similar technologies is regulated by the Law on Electronic Communications. According to this provision, necessary cookies/technologies can be used without consent. It is only necessary to inform the user, in a transparent manner, what cookies/technologies are used, their purpose, and their expiration.

The use of unnecessary cookies/technologies requires opt-in consent.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs are deemed similar to direct marketing; thus, the rules described in question 4.1 apply.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media channels are considered to be one of the public means of mass media. Thus, the Law on Public Information and the Law on Consumer Protection applies. According to these laws, hidden advertising is prohibited—social media influencers must use #reklama (#advertising) in each of their marketing posts.

In addition, it is prohibited to use an image of a person for commercial purposes without their consent.

Advertising in mass media (including social media channels) must comply with the following rules:

- (a) technologies which affect the subconscious mind cannot be used;
- (b) the advertisement cannot be misleading;
- (c) the dignity of a person cannot be humiliated;
- (d) discriminatory content is not allowed;
- (e) there must be no support or encouragement of dangerous behavior which can cause harm to a person;
- (f) advertising of tobacco products is prohibited;
- (g) no advertising of alcoholic beverages;
- (h) medicines can be promoted only in accordance with the Law on Pharmacy;
- (i) advertising which has a negative influence on those underage (ie, which harms their mental or physical health, or otherwise negatively impacts their development) is prohibited;
- (j) advertising of gaming is allowed only with certain harsh restrictions under the Law on Gaming (Note that, as of January 1, 2028, gaming advertising will be entirely prohibited) ; and
- (k) lotteries can only be advertised following the restrictions set out in the Law on Lotteries.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Please see question 7.1.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Not regulated locally.

7.7 How is location-based advertising regulated under privacy law?

Not regulated locally.

7.8 How are data brokers defined and regulated under privacy law?

Currently there are no specific legal rules governing the activities of data brokers in Lithuania.

7.9 How is advertising to children and minors regulated under privacy law?

There are two major requirements:

- (a) to conduct a privacy impact assessment; and
- (b) to comply with the Law on Protection of Minors Against Detrimental Effect of Public Information. This law prohibits dissemination of any information which is, inter alia:
 - (i) of a violent nature;
 - (ii) encouraging aggression and disrespect for life;
 - (iii) encouraging the destruction or damage of property;
 - (iv) showing a close-up view of the body of a dead, dying or severely injured person, except in cases where such a display is necessary to identify the person;
 - (v) showing content of an erotic nature;
 - (vi) showing content causing fear or horror, etc.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There is no specific local regulation, GDPR rules apply. See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

To the best of our knowledge, no.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Data transfers are governed by GDPR principles and rules. See the European Union chapter. The Local Privacy Law does not provide any additional restrictions.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Intra-group data transfer agreements and safety of data can be mentioned as other issues to consider when transferring data:

- (a) Belonging to the same group of companies does not, per se, mean that data can be shared. Group companies should agree on the necessity for data sharing, the scope of the data to be shared, the legal grounds, purposes of further data use, allocation of responsibilities towards data subjects, etc. This is usually done by signing an Intra-group Data Sharing Agreement.
- (b) Data transfers to third parties need to be safe. Sending data by email is not a safe way to transfer personal data. Thus, additional technical measures, such as encryption, password protection, using VPN, using 'do not forward' function, etc must be applied.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Lithuania? Are there minimum standards? Does this differ by sector or size of the entity?

Currently there are no minimum standards or security measures which should be implemented in order to ensure security of data. However, based on the requirements of the GDPR, all companies processing data should perform a risk assessment. Based on the findings of such risk assessment, a list of adequate security measures must be approved and implemented in the company.

The Lithuanian supervisory authority has introduced an IT risk assessment template for small and medium-sized companies. It can be found online at <https://vdai.lrv.lt/>.

9.2 How are personal data breaches regulated in Lithuania? What are the requirements for notification and response?

The Local Privacy Law does not specifically regulate data breach handling procedures; thus, the GDPR rules apply. See the European Union chapter. In summary, a data controller which has suffered a data breach must inform the supervisory authority within 72 hours. A model data breach notification for the Lithuanian supervisory authority can be found at <https://vdai.lrv.lt/>.

In addition, a company which suffered a data breach must assess the potential risks for data subjects and, when the risk is high, data subject must also be informed.

In practice, many companies engage external cybersecurity forensic specialists, privacy lawyers and PR specialists, and call centers which help manage the incidents. However, please note that there is no legal obligation to engage such external advisors.

According to the Law on Cyber Security (implementing the NIS2 directive), companies which are considered as 'important' or 'essential' must also inform the Center on Cyber Security.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

In Lithuania, the highest monetary fine for breach of GDPR rules so far is €2.34 million. The fine was imposed on Vinted—a marketplace for the sale of pre-owned clothing. The fine was imposed mainly for the failure to implement a right to be forgotten, failure to implement the principle of accountability and for the shadow banning techniques used on the platform.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, individuals have a right to file a civil claim and to ask for compensation for material and non-pecuniary damages. Usually, the courts award rather small amounts per individual for non-pecuniary damages (up to €300 in recent data breach cases, which did not involve special categories of data).

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Two local supervisory authorities (the State Data Protection Inspectorate and the State Consumer Rights Protection Authority) are very active in terms of privacy related matters. Most privacy-related claims are investigated and, if the claims are valid, end in either a reprimand or a fine. In 2024, the authority received around 1,400 claims, 1,081 claims were investigated and about a quarter ended in a fine or a reprimand. More statistics can be found in the annual report of the supervisor.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Lithuania?

In Lithuania, people are very sensitive about the processing of their personal code (see question 3.2). The Local Privacy Law even includes a prohibition on using personal code for the purposes of advertising.

Lithuanian people are also traditionally 'sensitive' to religion questions (the majority of the population is Roman Catholic).

LGBTQ+ is also a sensitive issue in advertising.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Currently, artificial intelligence is the hottest topic. Also, the NIS2 Directive is commonly discussed, as it has a significant impact on various business sectors, including advertising.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

In Lithuania, companies have a tradition of congratulating people on their birthdays, giving presents or otherwise celebrating this personal event. It is difficult for companies to understand that such data processing may lack a legal ground, and that the legitimate interest of the company will most likely not override the privacy of the person in this regard.

There is a statutory prohibition on processing criminal background data and credit rating for the purposes of employment (a few exceptions apply).

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

- (a) The biggest change was brought about as a result of artificial intelligence technologies. AI is now widely used for marketing campaigns, which creates new legal and compliance issues.
- (b) The war in Ukraine is still very significant in Lithuania, because governmental institutions and public entities (especially those managing critical infrastructure) have experienced multiple organized cyber-attacks since the beginning of the war.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenge is human inflexibility—it is really difficult to change behavior which has been carried on in the wrong way for many years into new privacy-friendly behavior.

12.3 What do you envision the privacy landscape will look like in five years?

- (a) Privacy documentation will be deregulated (as per Draghi's Report on the future of European competitiveness).
- (b) The Lithuanian online police forces will be expanded and will be able effectively to tackle unlawful behavior in social media and other online spaces.
- (c) The Meta world will present new challenges in terms of Meta identity and data protection in the virtual universe.

 LUXEMBOURG

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Luxembourg.

Privacy in Luxembourg is regulated by EU laws (notably the GDPR) and statutory law. The GDPR has been directly applicable in Luxembourg as of May 25, 2018.

Prior to the entry into force of GDPR, the main source for privacy law in Luxembourg was the Law of August 2, 2002 (as amended) concerning the protection of individuals with regard to the processing of personal data. This Law transposed the Data Protection Directive 95/46/EC into national legislation.

The Law of August 1, 2018 on the organization of the National Data Protection Commission and the general data protection framework ('Law of August 1, 2018') repeals the Law of August 2, 2002 and completes the GDPR at the national level. This law entered into force on August 20, 2018. The Luxembourg legislator mainly focused on implementing some opening clauses, rather than imposing additional restrictions on the processing of personal data.

In the field of criminal and national security matters, the Luxembourg legislator adopted a separate act (Act of August 1, 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters) to transpose the EU Police and Law Enforcement Directive 2016/680 into national law.

In addition to the general data protection legislative framework, sector-specific laws, as well as general guidance issued by the Luxembourg Supervisory Authority, cover the processing of certain categories of data (eg, processing of health data, processing for anti-money laundering purposes, processing of passenger name records data, processing in the context of social elections). The processing of health data in the context of insurance is currently the subject of a new bill.

The Luxembourg supervisory authority is the National Data Protection Commission ('CNPD'). The CNPD is responsible for monitoring and verifying that personal data are processed in compliance with data protection laws and notably the GDPR.

1.2 What are the primary laws regulating privacy in Luxembourg? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) **GDPR:** This is the main source for data protection in Luxembourg.
- (b) **The Law of August 1, 2018:** This completes the GDPR at national level and implements some opening clauses, namely rules for the following specific types of processing:
 - (i) Personal data processing for the purposes of surveillance in the employment context;
 - (ii) Processing for the sole purpose of journalism or academic, artistic or literary expression: in such cases controllers are exempt from:
 - prohibition on processing special categories of personal data,
 - the limitation on processing public judicial data
 - the rules applicable to transfers to third countries,
 - the obligation to provide certain information to the persons concerned, and
 - the obligation to give access to data subjects in certain circumstances.

- (iii) Processing for the purposes of scientific or historical research or statistical purposes: in such cases, provided that, inter alia, a data protection officer is appointed and impact assessment carried out, the data controller may:
 - limit the data subjects' rights to access, rectification, restriction of processing and objection where they would prevent or seriously impair the realization of the research project, and
 - process special categories of personal data necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes; and
- (iv) Processing of special categories of personal data: The processing of genetic data for the purposes of the exercise of the specific rights of the controller in the field of labor law and insurance is prohibited.

These rules on the specific processing purposes apply to all data controllers and data processors established in Luxembourg.

E-privacy aspects are regulated in Luxembourg by two main instruments:

- (c) the amended Act of May 30, 2005 concerning the specific provisions for protection of the individual in respect of the processing of personal data in the electronic communications sector, and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure (**'ePrivacy Law'**); and
- (d) the law of August 14, 2000 on electronic commerce (**'Electronic Commerce Law'**).

See, further, question 7.1.

For other sector-specific laws, see question 1.1.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Commission Luxembourgeoise pour l'Ethique en Publicité ('CLEP') acts as a self-regulatory body in Luxembourg for the advertising sector. CLEP aims to maintain standards of loyalty and ethics for advertising in all media throughout the Grand-Duchy of Luxembourg. CLEP has enacted a Code of Ethics which sets out non-compulsory general guidelines relating to advertising (the 'Advertising Code of Ethics'). The Advertising Code of Ethics specifically regulates online behavioral advertising (see question 7.5).

1.4 How is privacy law enforced in Luxembourg? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

(a) Regulators

- (i) Data protection laws are enforced by the CNPD and by the state courts. Under the Law of August 1, 2018, the CNPD has all the investigative, corrective, authorization and advisory powers referred to in the GDPR and may impose administrative fines and order, at the expense of the person sanctioned, the complete or partial publication of its decisions.

The CNPD has the power to bring any infringements of the GDPR and/or of the Law of August 1, 2018 to the attention of judicial authorities and, where applicable, the power to initiate legal proceedings in connection with such infringements.

An appeal against the decisions of the CNPD taken pursuant to the Law of August 1, 2018 can be made before the Administrative Tribunal, which rules on the merits of the case.

- (ii) For audiovisual media services (TV and VOD), video sharing platform services, and radio services, the Luxembourg Authority for Independent Audiovisual ('ALIA') monitors programs broadcast by audiovisual media services under its jurisdiction to ensure they:
 - respect human dignity;
 - contain no incitement to violence or hatred;
 - contain no public incitement to commit a terrorist offence;
 - comply with provisions concerning the protection of minors;
 - comply with all obligations relating to commercial communications.

In this context, the ALIA may cooperate with the CNPD for privacy concerns.

- (iii) In the context of the EU Digital Service Act ('DSA'), the Luxembourg Competition Authority has been designated as national digital services coordinator, overseeing compliance with the DSA, targeting online platform advertising.

(b) Self-regulatory bodies

There is no self-regulatory body responsible for the enforcement of privacy laws in general.

In the field of advertising, CLEP is responsible for enforcing the provisions of the Advertising Code of Ethics (including those on online behavioral advertising).

CLEP advises the advertising community and handles complaints. It is also entitled to act on its own initiative. CLEP can ask for modifications or decide to ban an advertisement, but its decisions are only binding on members of the Luxembourg Advertising Council (any advertiser may become a member of the CLP provided a membership fee is paid).

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Luxembourg?

See the European Union chapter.

2.2 Does privacy law in Luxembourg apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

As to the provisions of the GDPR, see the European Union chapter.

The rules on specific processing purposes under the Law of August 1, 2018 (see question 1.2(b)) apply only to data controllers and data processors established in Luxembourg.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Luxembourg?

See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

The processing of genetic data for the purposes of the exercise of the specific rights of the controller in the field of labor law and insurance is prohibited. For specific processing purposes, see question 1.2(b).

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

In addition, in March 2019, the CNPD published a list of the types of processing operations which are subject to the requirement for a data protection impact assessment ('DPIA') under the GDPR. This list is non-exhaustive and includes the following processing operations:

- (a) processing involving genetic data, in combination with at least one other criterion contained in the European Data Protection Board's adopted guidelines on DPIAs (the 'Guidelines'). Health professionals providing health services are not subject to this requirement;
- (b) processing that includes biometric data for the purpose of identifying data subjects, in combination with at least one other criterion contained in the Guidelines;
- (c) processing involving the combination, matching or comparison of personal data collected from processing operations with different purposes (from the same or different controllers) which produce legal effects or have a similar significant impact on the data subject;
- (d) processing which consists of, or includes, regular and systematic monitoring of employees' activities, and which may produce legal or similar significant effects with regard to employees;
- (e) processing of files likely to contain personal data of the entire national population (except where a DPIA has already been carried out as part of a general impact assessment);
- (f) processing for scientific or historical research purposes or for statistical purposes as provided for in the Law of August 1, 2018;
- (g) systematic monitoring of the location of natural persons; and
- (h) processing based on the indirect collection of personal data in conjunction with at least one other criterion contained in the Guidelines, where it is neither possible nor feasible to guarantee the right to information.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications are regulated by GDPR rules (see the European Union chapter).

In addition, commercial communications are regulated by Electronic Commerce Law and ePrivacy Law. The Electronic Commerce Law defines ‘commercial communications’ as any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing a commercial, industrial or craft activity or exercising a liberal profession. Information allowing direct access to the activity of the company, organization or person, (such as a domain name or an email address), or communications relating to the goods, services or image of the company, organization or person compiled in an independent manner, particularly when this is without financial consideration do not, in themselves, constitute commercial communications.

Commercial communications must comply with the following requirements:

- (a) they must be clearly identifiable as such;
- (b) the natural or legal person on whose behalf they are made must be clearly identifiable; and

- (c) promotional contests, offers or games must be clearly identifiable as such, and their conditions of participation must be easily accessible and presented in a precise and unambiguous manner.

Unsolicited commercial communications by electronic mail must be identifiable clearly and unambiguously on receipt by the recipient. The practice of sending electronic mail for purposes of direct marketing, disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, is prohibited.

When sending unsolicited commercial communications to natural persons, the general rule is that prior consent of the recipient is required ('opt-in' mechanism).

However, there is an exception ('opt-out' mechanism), where a natural or legal person obtains electronic contact details from its customers in the context of the sale of a product or a service, that person may use the electronic contact details for direct marketing of its own similar products or services, provided that customers are, clearly and distinctly, given the opportunity to object, free of charge and in an easy manner, to such use of their details, both when they are collected and on the occasion of each message. This exception must be interpreted restrictively.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

The Advertising Code of Ethics specifically regulates the online behavioral advertising.

Online behavioral advertising must be clearly identifiable as such. The use of a specific symbol which is apparent, distinguishable from the content of the message and perfectly visible and legible, should make it possible to inform the public about the behavioral nature of advertising.

A dedicated space should also provide the public with clear information on the different possibilities for refusing or accepting the display of behavioral advertising, including the modalities:

- (a) to consent to cookies;
- (b) to delete cookies; and
- (c) to object to the display of any behavioral advertising ('opt-out' systems).

Professionals should refrain from creating specific categories of advertising appealing to the interests of children of 12 years or under.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Luxembourg? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

In addition, there are some sector-specific standards:

- (a) **Electronic communications sector:** The ePrivacy Law implementing the EU ePrivacy Directive, imposes specific security obligations on providers of publicly available electronic communications services. These providers must ensure the security of their networks and services, including protecting personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

- (b) **Operators of essential services and digital service providers:** The Law of May 28, 2019 transposes the EU NIS Directive into Luxembourg law, requiring these entities to take appropriate and proportionate technical and organizational measures to manage risks posed to the security of network and information systems.
Luxembourg is in the process of transposing the NIS2 Directive into national law. The draft bill aims to enhance cybersecurity requirements across various sectors, including stricter obligations for risk management, incident reporting, and supply chain security. Once enacted, this legislation will impose more rigorous standards on entities operating in critical sectors.
- (c) **Financial and Insurance sectors:** The Law of July 1, 2024 ensures the effective application and enforcement of the Digital Operational Resilience Act ('DORA') in Luxembourg and provides for ICT risk management, incident reporting, digital operational resilience testing, third party risk management and information sharing.

9.2 How are personal data breaches regulated in Luxembourg? What are the requirements for notification and response?

See the European Union chapter.

In the event of a personal data breach, data controllers must notify the CNPD without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it must be accompanied by reasons for the delay.

When a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must also communicate the breach to the affected data subjects without undue delay. However, this communication is not required if the controller has implemented appropriate technical and organizational protection measures (eg, encryption) that render the data unintelligible to unauthorized persons.

Moreover, providers of publicly available electronic communications services must notify the CNPD of a personal data breach no later than 24 hours after detection. If the breach is likely to adversely affect the personal data or privacy of subscribers or individuals, the provider must also notify the affected parties without undue delay.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The CNPD has imposed the following sanctions:

- (a) **Law of August 1, 2018:**
 - (i) For delay in complying with an order by the CNPD to provide information or with a corrective measure enjoined by the CNPD: the CNPD has the power to impose periodic penalty payments of up to 5% of the average daily turnover generated by the data controller or data processor during the last financial year per day of delay;
 - (ii) Any person who willfully prevents or impedes, in any way, the execution of the tasks of the CNPD may be sentenced to imprisonment for a period of between 8 days and 1 year and/or a fine of €251–125,000; and

- (iii) Violation of the rules on the processing of an employee's personal data for surveillance purposes may result in a fine of up to €125,000 and/or imprisonment of up to one year.
- (b) **GDPR:**
 - (i) The CNPD launched a global campaign targeting DPOs that had been appointed in several companies in both the private and public sectors. DPOs were requested to fill in a questionnaire on their functions. Based on their answers, the CNPD initiated further investigations, which led to sanctions. Administrative fines ranging from €6,600–135,000 were given as well as reminders and injunctions to comply with the CNPD's order within 2–6 months.
 - (ii) The CNPD has also investigated the compliance with CCTV obligations in many companies. It appears that many entities experienced difficulties to fulfil their obligations regarding information, data minimization, and security of processing. These investigations led to administrative fines ranging from €200–12,500. (Note that, in order to comply with the duty of information in the context of CCTV, the CNPD considers it a matter of good practice to give data subjects a primary level of information together with a QR code that redirects data subjects to the privacy policy as a second level of information.)
 - (iii) An administrative fine amounting to €1,000 has been issued against a public institution regarding the right to erasure of data.
 - (i) In 2023, the CNPD sanctioned several municipalities for failing to appoint DPOs and not communicating their contact details.
 - (ii) In 2025, the CNPD has imposed a record fine of €746 million on Amazon Europe Core Sàrl for violations of the GDPR. In 2021, An action was initiated by the digital rights advocacy group 'la Quadrature du Net', representing over 10,000 individuals about targeted advertising practices that claims lacking valid consent and transparency. The CNPD's investigation concluded that Amazon:
 - processed personal data for interest-based advertising without obtaining valid user content, relying instead on 'legitimate interest', which was deemed insufficient given the nature of the processing;
 - -provided inadequate and unclear information about data processing activities and violating transparency obligations;
 - failed to adequately address data subject's rights, such as access, rectifications, erasure and objection.

Amazon challenged the CNPD's decision, but on 18 March 2025, the Administrative Court of Luxembourg upheld the CNPD's initial decision by emphasizing that Amazon's reliance on legitimate interest did not justify the extensive data processing for personalized advertising, especially in the absence of explicit user consent. A further appeal on the decision may be pending.

See also the European Union chapter.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The CNPD has demonstrated a proactive stance in enforcing privacy regulations, particularly in the Amazon case (see question 10.1.)

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Luxembourg?

None.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Advertising companies operating in Luxembourg must navigate a rapidly evolving regulatory landscape shaped by both national enforcement priorities and EU-level legislation among which the following topics should be monitored closely:

- (a) **Targeted advertising and consent management:** Many advertisers still rely on ‘legitimate interest’ to justify targeted advertising, but recent enforcement, such as the Amazon case, shows that regulators expect explicit opt-in consent.
- (b) **Advertising to children and minors under the Digital Services Act (‘DSA’):** Targeted ads to minors are prohibited; however, there is still a lack of robust age-verification mechanisms that could expose companies to liability.
- (c) **Influencer and native advertising transparency:** Social media ads and sponsored content often blur the line between editorial and commercial speech. The ALIA (Luxembourg’s audiovisual regulator) is expected to increase oversight of influencer marketing and audiovisual content.
- (d) **Use of AI in advertising:** Personalized content and predictive analytics powered by AI are gaining ground, but the EU AI Act (expected to apply from 2026) classifies some advertising-related AI (eg, manipulative targeting) as high-risk or prohibited.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

After the entry into force of the GDPR, the CNPD published several guidelines clarifying certain sensitive privacy issues (video surveillance, social elections, dashcams, the right of publicity etc). While not binding, these guidelines will most likely be the main source for the courts when interpreting GDPR provisions. Therefore, companies should make sure their processing activities comply with CNPD guidelines.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, Luxembourg’s privacy landscape has undergone significant transformations, driven by both national initiatives and broader EU regulatory developments. These changes have been propelled by technological advancements, heightened enforcement activities, and the introduction of new legal frameworks:

The CNPD has conducted several thematic investigations into the transparency of data processing information provided by web services, emphasizing the need for clear, concise, and accessible privacy notices.

To support organizations and adapt to technological advancements, the CNPD has launched several initiatives:

- (a) **Certification:** In May 2022, the CNPD introduced GDPR-CARPA, the first national and international certification mechanism under the GDPR. This scheme allows organizations to demonstrate compliance with data protection standards;
- (b) **DAAZ Platform:** An e-learning platform named 'Data Protection from A to Zen' ('DAAZ') has been developed to assist organizations in understanding and complying with GDPR requirements; and
- (c) **AI Sandbox:** The CNPD has introduced a regulatory sandbox dedicated to artificial intelligence, allowing for the testing of AI systems in a controlled environment to ensure GDPR compliance.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The patchwork of new legislations and regulatory layers are forcing companies to step up their compliance levels. The evergreening of new technologies and the use of responsible, reasonable and trustworthy AI remains a challenge.

The EU AI Act is highly relevant, and is poised to significantly influence the country's privacy and regulatory landscape. Luxembourg is actively implementing the AI Act through Draft Law No 8476, introduced on December 23, 2024, which establishes national authorities, enforcement mechanisms, and regulatory sandboxes to align with the EU's AI framework. It represents a significant development in the country's regulatory framework, emphasizing ethical AI development, sector-specific oversight, and the integration of data protection principles. Organizations operating in or targeting the Luxembourg market should closely monitor these developments to ensure compliance and leverage opportunities for innovation within the regulatory sandboxes.

12.3 What do you envision the privacy landscape will look like in five years?

Over the next five years, Luxembourg's privacy landscape will be shaped by complex technological advancements, deep integration of AI, stricter consent requirements, cross-regulation enforcement, and a shift toward ethical and privacy-preserving digital marketing.

Complex legal overlap will therefore pose challenge compliance (GDPR, the AI Act, the DSA etc) guided by transparency principles, explainability, ethical and trustworthiness.

Environmental and ethical marketing may also be impacted by the proposed EU Green Claims Directive.

 MALTA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Malta.

Privacy in Malta is primarily governed by the General Data Protection Regulation ('GDPR'), which applies directly across all EU Member States, including Malta. The GDPR is supplemented by the Maltese Data Protection Act (Chapter 586 of the Laws of Malta), which provides for the establishment and powers of the Information and Data Protection Commissioner ('IDPC') and addresses areas not fully harmonized by the GDPR.

1.2 What are the primary laws regulating privacy in Malta? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary laws include:

- (a) GDPR (Regulation (EU) 2016/679)
- (b) Data Protection Act (Cap. 586)
- (c) ePrivacy Regulations (SL 586.01)
- (d) Sector-specific laws such as the Financial Institutions Act and the Gaming Act.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays a limited role. While industry codes of conduct are encouraged under Article 40 GDPR, Malta has not yet adopted sector-specific codes for advertising. However, companies often follow best practices aligned with EU-wide standards, such as those from the European Advertising Standards Alliance ('EASA').

1.4 How is privacy law enforced in Malta? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The IDPC is Malta's supervisory authority. It investigates complaints, conducts audits, and issues administrative fines. Enforcement is generally aligned with GDPR principles, and the IDPC has the authority to impose corrective measures, including warnings, reprimands, and fines.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Malta?

Any entity processing personal data in the context of an establishment in Malta is subject to Maltese data protection law. This includes both controllers and processors.

2.2 Does privacy law in Malta apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The GDPR applies extraterritorially. Non-EU companies targeting Maltese data subjects or monitoring their behavior must comply and appoint an EU representative, who may be based in Malta if the data subjects are located there.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Malta?

'Personal data' is defined as any information relating to an identified or identifiable natural person (data subject), including names, identification numbers, location data, and online identifiers.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Special categories include:

- (a) data revealing racial or ethnic origin;
- (b) data revealing political opinions, religious beliefs;
- (c) data revealing trade union membership;
- (d) genetic and biometric data;
- (e) health data; and
- (f) data concerning sex life or sexual orientation.

Processing is prohibited unless specific conditions under the GDPR are met.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized data falls outside the GDPR. Pseudonymized data remains personal data if re-identification is possible, and must be protected accordingly.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must:

- (a) ensure transparency and lawful processing;
- (b) provide privacy notices;
- (c) facilitate data subject rights;
- (d) maintain records of processing;
- (e) implement appropriate security measures; and
- (f) conduct data protection impact assessments ('DPIA's) where required.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Controllers determine the purpose and means of processing; processors act on behalf of controllers. Obligations differ, particularly regarding contracts and accountability.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Processing must be based on one of the lawful bases under the GDPR: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Notices must include:

- (a) the identity of the controller;
- (b) purposes of processing;
- (c) legal basis;
- (d) recipients;
- (e) data subject rights; and
- (f) information on international transfers.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the following rights:

- (a) access;
- (b) rectification;
- (c) erasure;
- (d) restriction;
- (e) portability;
- (f) objection; and
- (g) not to be subject to automated decision-making.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Consent must be freely given, specific, informed, and unambiguous. For electronic marketing, prior opt-in consent is required unless the soft opt-in exemption applies.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Controllers must ensure processors provide sufficient guarantees and enter into data processing agreements ('DPA's) under the GDPR.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

DPAs must specify:

- (a) subject matter;
- (b) duration;
- (c) nature;
- (d) purpose;
- (e) type of data;
- (f) categories of data subjects; and
- (g) obligations of both parties.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Due diligence includes assessing vendor security, compliance history, and conducting DPIAs for high-risk processing, including advertising profiling.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing is regulated under the ePrivacy Regulations.

Consent is required for unsolicited communications unless the soft opt-in applies.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Cookies and similar technologies require prior consent unless strictly necessary.

Transparency and opt-out mechanisms are essential.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions must comply with GDPR principles.

Consent is required for profiling or marketing beyond the program's core function.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing are subject to GDPR and ePrivacy rules.

Transparency, lawful basis, and disclosures are key.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising requires consent or legitimate interest with a balancing test.

Contextual advertising may not involve personal data, and thus may fall outside the GDPR.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are subject to the GDPR if personal data is involved.

DPIAs and contractual safeguards are recommended.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising requires explicit consent due to the sensitivity of location data.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are not specifically regulated, but are subject to the GDPR.

Transparency and lawful basis are required.

7.9 How is advertising to children and minors regulated under privacy law?

Children merit specific protection. Parental consent is required for services offered directly to children under 16 (or 13, if national law allows).

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Automated decision-making with legal or significant effects requires explicit consent or other safeguards as provided by the GDPR.

7.11 Are there other specific advertising practices that you wish to discuss?

Use of dark patterns or manipulative consent mechanisms is discouraged, and may be deemed non-compliant.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The transfer of personal data is permitted to countries with an adequacy decision. Otherwise, standard contractual clauses ('SCC's), binding corporate rules ('BCR's), or derogations must be used.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Transfers must be documented and assessed for risk. Legal privilege and sector-specific rules may apply.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Malta? Are there minimum standards? Does this differ by sector or size of the entity?

Controllers and processors must implement appropriate technical and organizational measures. There are no sector-specific minimums, but ISO standards are often referenced.

9.2 How are personal data breaches regulated in Malta? What are the requirements for notification and response?

The supervisory authority must be notified within 72 hours of becoming aware of a breach, unless the breach is unlikely to result in risk. Data subjects must be informed if there is a high risk.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Fines of up to €20 million or 4% of global annual turnover, whichever is higher, may be imposed, depending on the nature and severity of the breach.

10.2 Do consumers have a private right of action? What remedies are available to them?

Data subjects may lodge complaints with the IDPC or seek judicial remedies, including compensation for material and non-material damage.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The IDPC has issued fines and warnings, particularly in the areas of marketing, data breaches, and failure to respond to data subject requests.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Malta?

Malta's small size and close-knit business community often lead to heightened reputational risks for non-compliance.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Hot topics include:

- (a) AI regulation and its intersection with the GDPR;
- (b) cookie compliance and enforcement; and
- (c) cross-border enforcement cooperation

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Controllers should monitor European Data Protection Board ('EDPB') guidance and European Court of Justice ('CJEU') rulings, which directly impact Maltese practice.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There has been increased enforcement focus on transparency, cookies, and legitimate interest assessments. This has been triggered by EDPB guidance and high-profile CJEU decisions.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenges companies face due to the changing privacy landscape are:

- (a) managing cross-border data flows post-Schrems II;
- (b) aligning marketing practices with consent requirements; and
- (c) keeping up with evolving regulatory guidance.

12.3 What do you envision the privacy landscape will look like in five years?

In five years we would expect:

- (a) greater harmonization of enforcement across the EU;
- (b) increased scrutiny of AI and profiling; and
- (c) a shift toward proactive compliance through certification and codes of conduct.

 NETHERLANDS

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in the Netherlands.

Privacy is regulated on two levels in the Netherlands: on the level of the European Union and on national level.

On the level of European Union, the EU General Data Protection Regulation ('GDPR') is the most important applicable source of law, which covers all aspects of privacy law concerning the processing of personal data. See the European Union chapter for further information on privacy regulations on EU level.

On the national level, privacy is regulated in a couple of difference sources. The right to privacy has been part of the Dutch Constitution since 1983 and is described as the right to respect for one's private life. This right encompasses privacy in the home, regarding correspondence, communication by telephone, telegraph and other private means of communication, the right to not be watched or overheard in private situations, the right to careful treatment of personal data, and the right to respect for inner life and physical integrity. Several of these aspects of privacy have a specific constitutional guarantee in other Articles of the Dutch Constitution.

Moreover, the Constitution requires the establishment of laws that provide rules for the protection of private life regarding the recording and provision of personal data and regulate the right of access to and the right to correct inaccurate personal data. The GDPR accommodates most of the legislation required, with further aspects covered, inter alia, by the Dutch GDPR Implementation Act ('Implementation Act').

A final source of law that governs data protection in the Netherlands is the Dutch Telecommunications Act. The Telecommunications Act is derived from the ePrivacy Directive and governs data protection aspects such as cookies. Once the ePrivacy Regulation comes into force, it will replace the Telecommunications Act (but note that the European Commission has withdrawn the proposal for the ePrivacy Regulation, and efforts to modernize the ePrivacy Directive have been shelved for the time being).

1.2 What are the primary laws regulating privacy in the Netherlands? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The GDPR forms the primary source for data protection in the European Union and therefore in the Netherlands. See European Union chapter.

The Implementation Act broadly covers two topics:

- (a) it establishes the position and powers of the Dutch data protection authority ('AP') as the supervisory authority;
- (b) it gives substance to the opening clauses regarding the special categories of personal data.

Certain aspects of marketing activities, including direct marketing by email or telephone and the use of cookies and similar tracking technologies (eg for targeted advertising) are regulated in the Telecommunications Act (see question 7.1 and 7.2).

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Netherlands does not have any self-regulatory bodies that enforce privacy law.

However, a relevant self-regulatory framework exists in the field of advertising: the Dutch Advertising Code, enforced by the Advertising Code Committee through non-binding rulings (recommendations) issued in response to complaints.

Several special advertising codes, which are part of the Dutch Advertising Code, address direct marketing practices involving personal data, including the Code for Distribution of Advertisements by Email ('Email Code') 2012, the Telemarketing Code 2024, the Letter Box Advertising, Door-to-Door Sampling and Direct Response Advertising Code, and the Advertising Code for the use of the Postal Filter 2025. The Email Code and Telemarketing Code largely reflect the rules set out in the Telecommunications Act, with practical elaborations and some additional obligations.

1.4 How is privacy law enforced in the Netherlands? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Netherlands has only one data protection authority, the AP. The AP is tasked with monitoring the GDPR, the Implementation Act, and other laws protecting personal data. In case of a breach of the provisions of the GDPR, the AP is authorized to impose administrative fines. The Implementation Act does not grant the AP any powers beyond those set out in the GDPR.

As indicated in questions 1.1 and 1.2, certain privacy aspects are regulated outside of the GDPR and Implementation Act, in the Telecommunications Act. The supervisory authority for the Telecommunications Act (amongst others) is the Authority for Consumers and Markets ('ACM'). The ACM can impose fines for breach of the Telecommunications Act.

Private enforcement is also possible: individuals whose data protection rights have been violated can lodge complaints with the AP or bring civil claims for damages or injunctive relief before the courts. Additionally, representative actions (eg by consumer organizations or privacy NGOs) may be brought under Dutch class action procedures. See the European Union chapter.

Although the Netherlands does not have self-regulatory bodies that enforce privacy law, a relevant self-regulatory framework exists via the Dutch Advertising Code, which is enforced by the Advertising Code Committee through non-binding rulings. In the context of privacy, this self-regulation primarily concerns direct marketing practices involving personal data, such as email advertising and telemarketing. See question 1.3.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in the Netherlands?

See European Union chapter.

In addition to the applicability of the GDPR, the Implementation Act applies to companies which control or process personal data and are established in the Netherlands, irrespective of whether or not the data subjects are in the European Union. The Implementation Act also applies to companies established outside the European Union if the processing of personal data is linked to activities in the Netherlands (see question 2.2).

2.2 Does privacy law in the Netherlands apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law applies to companies outside the Netherlands on the basis of:

- (a) the GDPR: in situations where the GDPR is applicable, it applies to companies outside the Netherlands (see European Union chapter);
- (b) the Implementation Act: the Implementation Act applies to controllers and processors that are not established in the European Union, if the processing of personal data of data subjects in the Netherlands is linked to:
 - (i) offering goods and services to data subjects in the Netherlands, regardless of whether a payment by the data subjects is required; or
 - (ii) monitoring the behavior of such data subjects, insofar as this behavior takes place in the Netherlands.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in the Netherlands?

‘Personal data’ is defined by the GDPR (see European Union chapter).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The categories of personal data that are considered sensitive can be found in the GDPR. See the European Union chapter for comments on these categories. There are no specific obligations around sensitive information, other than the obligations in the GDPR.

However, in addition to the exemptions under the GDPR, the Implementation Act provides national exceptions that further specify or permit the processing of sensitive data in certain contexts. These include processing:

- (a) required by international obligations or for official tasks of the AP or an ombudsman;
- (b) for scientific or historical research or statistical purposes, subject to safeguards;
- (c) data revealing racial or ethnic origin for identification or to promote equal treatment;
- (d) political opinions in relation to public appointments;
- (e) religious or philosophical beliefs for the provision of spiritual care;
- (f) genetic data in the context of healthcare or research serving a public interest or for statistical purposes;
- (g) biometric data for authentication or security purposes;
- (h) of health data in healthcare, employment, education, justice, and insurance contexts.

Moreover, in addition to the general restriction in the GDPR, the Implementation Act lays down specific national rules for the processing of personal data relating to criminal convictions and offences.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The Netherlands follows the framework set out in the GDPR with regard to anonymized, pseudonymized, and de-identified data, as described in the European Union chapter. There are no additional definitions or legal qualifications in Dutch national law. The AP follows the same approach: Anonymized data that cannot reasonably be re-identified is considered outside the scope of the GDPR.

and the Implementation Act. However, as under EU law, pseudonymized data remains subject to data protection rules as long as re-identification is reasonably possible.

The AP emphasizes that pseudonymization is a valuable security measure, particularly in high-risk processing or research contexts, but does not exempt data from the GDPR. The AP also notes that common techniques such as hashing do not always achieve true anonymization, especially if the original data or additional identifiers remain accessible, and because hash values can be reproduced.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

As outlined in the European Union chapter, the GDPR requires that all personal data processing be based on a valid legal basis. The Netherlands has not introduced additional lawful grounds for processing in the Implementation Act. However, the Implementation Act provides national specifications for how certain legal bases may be applied—particularly in areas such as healthcare, public administration, insurance, and the processing of special categories or criminal data (see question 3.2). It is also worth noting that, under the Implementation Act, the processing of national identification numbers is prohibited unless specifically permitted by law or carried out for purposes set out by law.

In addition, for unsolicited marketing communications and certain types of cookies, prior (opt-in) consent is generally required under the Telecommunications Act. see questions 7.1 and 7.2.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

In addition, under the Telecommunications Act, companies must provide clear and comprehensive information about the use of cookies and other tracking technologies, including their purposes (eg, advertising, analytics). This information is typically included in a cookie notice or cookie policy, which may be presented as part of the privacy notice.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

In addition, the Implementation Act provides for certain national exemptions and restrictions on data subject rights in specific contexts. While most of these apply to areas such as national security, journalism, scientific research, or public registers and are not generally relevant in advertising contexts, one exemption may be relevant: the Implementation Act contains an exemption to a data subject's right under the GDPR not to be subject to a decision based solely on automated processing, including profiling. The exemption applies to situations where automated individual decision-making (other than profiling) is necessary for compliance with a legal obligation to which the controller is subject, or for the performance of a task carried out for reasons of public interest.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

In addition, see questions 7.1 and 7.2 for an overview of how the opt-in system works in the Netherlands for unsolicited marketing communications, such as via electronic messages and phone calls, and for the use of cookies and other tracking technologies under the Telecommunications Act.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

The AP has published a non-exhaustive list of processing activities for which a DPIA is mandatory. This list includes processing activities such as profiling and the systematic observation or influencing of behavior, including the use of data for online behavioral advertising. Companies must consult the AP if high risks remain after a DPIA and no mitigating measures are available.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See European Union chapter for privacy law obligations.

The collection of personal data that will later be used for direct marketing purposes always requires a legal basis (eg consent). Which rules apply to the use of the personal data for direct marketing depends on the type of direct marketing, and whether or not the direct marketing is aimed at existing or future customers.

Different types of direct marketing can be identified, each subject to specific rules under the Telecommunications Act and the relevant advertising codes. In general, the same rules apply to digital direct marketing and telemarketing under the Telecommunications Act (though different specific requirements may apply under the relevant advertising codes), whereas different rules apply to advertising by post:

- (a) **Digital direct marketing and telemarketing:** The general rule is that unsolicited digital direct marketing can only be sent (by email, text or WhatsApp), and telemarketing regarding natural persons is only allowed, if prior consent has been obtained from the data subject.

There is one general exemption to this rule for both digital direct marketing and telemarketing, namely that permission is not required for offers aimed at existing customers (including former customers; however, for telemarketing, this only includes those who have been a customer within the past three years), provided that the offer concerns the company's own, similar products, the customer did not object to the use of their personal data for digital marketing or telemarketing at the time it was collected, and is given the opportunity to opt out with every subsequent message or call. For non-profit organizations, consent is not required for digital direct marketing and telemarketing if the data subject is a donor of the charity, has done voluntary work for them or has attended a meeting.

Two exemptions apply in the B2B context for both digital direct marketing and telemarketing. No prior consent is required when unsolicited commercial, charitable, or ideological communications are sent to or telemarketing calls are made to a legal entity or a natural person acting in the course of a profession or business, in case:

- (i) the electronic contact details used were explicitly made public by the recipient, and they are used in accordance with the purpose for which they were made public; or
- (ii) the recipient is located outside the European Economic Area ('EEA'), provided the message complies with the relevant national laws on unsolicited communications in the recipient's country.

In addition to their rights under the GDPR, the Telecommunications Act also provides data subjects with the right to object to the use of their personal data for digital direct marketing. Data subjects should be given a clear, explicit and free of charge opportunity to express their objection to processing every time they receive digital direct marketing. If the right is invoked the company is no longer allowed to send digital direct marketing to the data subject concerned.

In addition, calling anonymously, using pre-ticked boxes, and putting pressure on people into giving their consent is not allowed. Finally, consent needs to be specific and informed and data subjects must be able to withdraw their consent at any time.

Besides the provisions of the Telecommunications Act, the self-regulating Email Code and Telemarketing Code apply in these areas (see question 1.3). These advertising codes largely reflect the rules set out in the Telecommunications Act, with practical elaborations and some additional obligations.

- (b) **Advertising by post:** Different rules for advertising by post apply to existing customers and future customers. In general, no prior opt-in consent is required. However, if data subjects have invoked their right to object, it is no longer permitted to send them advertising by post, irrespective of whether they are existing or future customers:

- (i) **Existing customers:** Personal data of existing customers is most likely collected for processing purpose other than direct marketing. In order to process such personal data, it should be assessed whether or not the direct marketing purpose is compatible with the initial purpose. If the purposes are compatible, advertising by post can be sent to the data subject without prior consent. If the current purpose is not compatible, it is necessary to acquire prior consent of the data subject.
- (ii) **Future customers:** Advertising by post to future customers requires permission of the data subject, or a valid legitimate interest of the company. Recital 47 of the GDPR confirms that direct marketing can be considered a legitimate interest, but a proper balancing test is required.
- (iii) **Postfilter:** If a data subject is registered in the Postfilter registry, no advertising by post may be sent. Advertising by post can still be addressed to existing customers who are registered in the Postfilter registry. However, if they object to this practice the company must refrain from sending advertising by post.

The self-regulating Letter Box Advertising, Door-to-Door Sampling and Direct Response Advertising Code, the Advertising Code for the use of the Postal Filter 2025 and the Code for the Distribution of Unaddressed Printed Advertisements apply to advertising by post.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

The use of tracking technology is regulated in the Telecommunications Act, which implements the relevant provisions of the ePrivacy Directive, alongside the GDPR. The AP emphasizes that consent for non-essential cookies must be obtained prior to placement, be freely given, specific, informed and unambiguous. Cookie banners must provide clear choices (eg, accept/refuse on the same layer), use clear language, avoid pre-ticked boxes or dark patterns, not require extra clicks to refuse, and enable easy withdrawal of consent. Website visitors must be clearly informed about how and why cookies are used, and must be able to refuse such cookies without negative consequences. Importantly, separate consent is required for each distinct purpose. Legitimate interest instead of consent only applies to functional or limited analytics cookies. The AP has intensified its enforcement of cookie compliance since 2024, particularly targeting non-transparent banners and unlawful tracking.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter. Although not directly part of privacy law, in the Netherlands, social media advertising is also subject to the self-regulatory Advertising Code for Social Media & Influencer Marketing, which sets out how a relevant relationship between an influencer and an advertiser (eg, payment or free products) must be clearly disclosed—such as through recognizable hashtags like #ad or #sponsored, placed prominently in the post.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter. The AP emphasizes that processing personal data for targeted advertising (including behavioral or personalized advertising) typically requires explicit consent.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter. While the AP has not issued specific guidance on these technologies, it consistently emphasizes that combining data from different sources for marketing or profiling purposes generally requires explicit consent, and that reliance on legitimate interest for such purposes is strictly limited.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter. The AP places emphasis on the need for explicit and freely given consent for precise location tracking.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

The AP provides additional guidance on address and data trading. Entities receiving personal data from third parties (such as data brokers, list brokers or address traders) must ensure both that the source has a valid legal basis for sharing the data and that they themselves have a lawful basis for using it—typically consent, unless the processing is strictly compatible with the original purpose. The AP emphasizes that this compatibility test is strict, and that customer data sales usually require demonstrable consent. Even data from public sources requires a separate legal basis. Combating unlawful data trading is an explicit supervisory focus area for the AP.

A relevant case in this context is the Royal Dutch Lawn Tennis Federation (‘KNLTB’) ruling by the Court of Justice of the EU (‘CJEU’) of 4 October 2024, which arose from a dispute between the AP and the KNLTB, referred by the Amsterdam District Court. The case concerned the sale of KNLTB member data to a third party for direct marketing purposes. The AP had long maintained that marketing purposes can never constitute a legitimate interest, although the GDPR does allow for that possibility. The CJEU clarified that commercial interests may, in principle, qualify as a legitimate interest under the GDPR, but only if the processing passes the legitimate interest assessment.

In response, the AP has revised its position: such processing may be lawful if based on a commercial interest, but only if a careful balancing test is performed—particularly in contexts involving data brokers or the (re)sale of personal data, where factors such as the reasonable expectations of data subjects and the level of transparency are decisive. If the outcome of the balancing test shows that the privacy rights of data subjects outweigh the commercial interest in a specific case, explicit consent must be obtained before the data can be (re)sold or used—for example, for direct marketing purposes.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter. As noted in the European Union chapter, the GDPR allows Member States to set a lower age limit—down to 13—for children to give valid consent to the processing of their personal data. The Netherlands has not made use of this option: under the Implementation Act, the minimum age remains 16 years. This means that the consent of a parent or legal guardian is required for children under 16.

The AP places particular emphasis on the need for heightened protection of minors. It discourages the profiling or targeting of children unless demonstrably in the best interests of the child, and it requires that privacy information be provided in language that children can understand. This includes a clear explanation of the purposes for which personal data is processed.

In addition, advertising directed at minors must comply with the self-regulatory Code for Advertising directed at Children and Young People. This self-regulatory code stipulates that:

- (a) when collecting personal data of a child (a child being a person of 12 and under), all efforts must be made to inform the child and/or their parent(s) of the purpose of data collection, and, where commercial content is specifically directed at children or when otherwise child's details are deliberately collected, the information provided must be clear, easily accessible, and comprehensible for children;
- (b) in line with legal requirements, specific forms of elaborating personal details of a minor/young person under 16 require that the permission of the parent/caretaker be granted; and
- (c) when offering a game, prize, or other sales promotional activity, children may not be required to disclose more personal data than is strictly necessary to participate.

The AP has further flagged AI applications targeting children as a high-risk area. In 2023, it initiated investigations into apps and chatbots using generative AI aimed at minors, expressing concern about transparency, data retention, and children's ability to understand what happens to their data. The AP reiterated that digital services directed at children must apply enhanced safeguards and follow strict data minimization principles.

Finally, under the EU Digital Services Act ('DSA'), which applies across the EU including the Netherlands, additional rules apply for digital services used by minors. The DSA requires that online platforms accessible to minors must put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on their service. A key provision is that, if an online platform knows or can reasonably be certain that a user is a minor, it may not present advertising on their interface based on profiling. This means online platforms must avoid targeting underage users with personalized ads based on behavioral data, preferences, or online activity. The DSA also encourages child-friendly explanations of terms and conditions, and the use of age verification tools, parental controls and tools aimed at helping minors signal abuse or obtain support by providers of very large online platforms and of very large online search engines. While the DSA is not specific to the Netherlands, its obligations reinforce and complement national privacy standards for protecting children online.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See European Union chapter.

In addition, the Implementation Act contains an exemption to a data subject's right under the GDPR not to be subject to a decision based solely on automated processing, including profiling. The exemption applies to situations where automated individual decision-making (other than profiling) is necessary for compliance with a legal obligation to which the controller is subject, or for the performance of a task carried out for reasons of public interest. This national exemption is narrowly framed and does not generally apply to commercial advertising contexts, where profiling and AI-driven decision-making remain subject to the full set of GDPR safeguards as set out in the European Union chapter.

The AP has made clear that profiling is only permitted under the strict conditions of the GDPR. Organizations must have a valid legal basis. Explicit consent is usually the only appropriate legal basis for profiling in marketing. When profiling produces significant effects for individuals, the AP requires that:

- (a) data subjects are clearly informed that profiling is used, why it is used, and what the consequences are;
- (b) data subjects are given the right to human intervention, ie to have an automated decision reviewed by a person;
- (c) the data used is accurate, and that organizations implement strong safeguards to protect individuals' privacy rights;
- (d) a data protection impact assessment ('DPIA') is conducted, as profiling is on the AP's mandatory DPIA list;
- (e) a data protection officer is appointed when large-scale profiling is a core activity.

Furthermore, the AP points out that the DSA, effective since 17 February 2024, introduces stricter rules than the GDPR for profiling in advertising. In particular, the DSA prohibits profiling based on special categories of personal data, and profiling of minors for advertising on online platforms (see question 7.9).

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter. The AP has not issued country-specific prohibitions, but in practice, transfers to high-risk jurisdictions (eg, Russia, China) are expected to meet a very high threshold of legal and technical due diligence.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in the Netherlands? Are there minimum standards? Does this differ by sector or size of the entity?

See European Union chapter.

In order to help companies to address data security standards as prescribed in the GDPR, the AP has issued online guidance and Q&As on this topic and the topic of data breach registration.

9.2 How are personal data breaches regulated in the Netherlands? What are the requirements for notification and response?

See European Union chapter.

In addition, financial companies governed by the Financial Supervision Act are exempted from the requirement to notify the data subject in case of a data breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

The AP enforces the GDPR and has the authority to impose administrative fines and other sanctions for violations. The AP's fining policy distinguishes between organizations:

- (a) **Private entities:** Fines are calculated based on the European Data Protection Board Guidelines 04/2022 on the calculation of administrative fines under the GDPR, considering factors such as the nature, gravity, and duration of the infringement;
- (b) **Public authorities and individuals not acting on behalf of a company:** The AP applies its own fining policy rules, updated in 2023, which outline specific categories and corresponding fine ranges.

In addition to administrative penalties under the GDPR, Dutch national criminal law provides for criminal sanctions in certain cases of severe privacy violations, such as the intentional breach of professional or official confidentiality and (since January 2024) the collection or dissemination of personal data (doxing) with the intent to intimidate, cause serious nuisance, or hinder someone in the performance of their job or duties.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

In the Netherlands, in addition to filing a complaint with the AP, data subjects have a private right of action under the GDPR, and may claim compensation before the civil courts for material or non-material damage resulting from unlawful data processing. Dutch procedural law also enables collective redress under the Act on Collective Damages in Class Actions ('WAMCA'), allowing authorized interest groups or foundations to bring representative claims—particularly relevant in mass data breaches or unlawful online tracking cases.

In a pending case before the Rotterdam District Court involving Amazon, the court has referred preliminary questions to the CJEU on whether the GDPR allows consumer rights organizations to bring collective privacy actions without individual mandates from data subjects, as permitted under the WAMCA. This may clarify the scope of collective actions under EU law and their interaction with national procedural rules.

Dutch courts apply a case-by-case assessment when awarding damages, but recent rulings—aligned with CJEU case law—indicate a lower threshold for recognizing non-material harm under the GDPR (eg, substantiated fear of future misuse following a data breach), with compensation often granted in the range of €250–€300 for violations such as the unauthorized disclosure of health data.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

See the European Union chapter.

The AP actively enforces privacy laws, with a focus on online advertising, algorithmic systems, and large-scale data processing in both public and private sectors. In its 2024 annual plan, the AP identifies the following priority areas: Algorithms & AI, Big Tech, Data Trading, Freedom & Security, and the Digital Public Sector. Recent enforcement decisions of the AP and civil lawsuits in the Netherlands in privacy-related matters involving advertising include:

- (a) In 2024, Netflix was fined €4.75 million for failing to properly inform customers about how their personal data was used between 2018 and 2020;
- (b) In 2024, the AP imposed a €600,000 fine on AS Watson (Kruidvat) for placing tracking cookies collecting information about sensitive product searches (eg, pregnancy tests and medications) on its website without valid consent;
- (c) A class action against Google filed by Stichting Bescherming Privacybelangen is currently pending, focusing on large-scale profiling and commercial exploitation of user data; and
- (d) In a collective action against Amazon, the Rotterdam District Court has referred questions to the CJEU about whether the GDPR allows collective actions without individual mandates—a case centered on advertising-related data use and profiling (see question 10.2).

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in the Netherlands?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Some ‘hot topics’ and anticipated legal challenges include:

- (a) The DSA imposes transparency obligations on online platforms regarding advertising. It also prohibits profiling-based ads targeting minors and the use of sensitive personal data for advertising profiling-based ads on online platforms.
- (b) Subscription models requiring users to either accept tracking or pay a fee (eg, for ad-free access) are under increased scrutiny. In April 2025, the European Commission fined Meta €200 million for its ‘pay or consent’ model on Facebook and Instagram, concluding that it failed to provide users with a less personalized but equivalent alternative, as required under the EU Digital Markets Act (‘DMA’).
- (c) The EU AI Act introduces additional obligations for AI systems, including those used in advertising and targeting. Companies deploying AI across the EU will likely navigate strict rules on data usage, transparency, and risk management, especially for high-risk AI systems. The interplay between the AI Act and the GDPR, particularly for cross-border contexts, means companies will face a more complex and demanding regulatory landscape.
- (d) The proposed Digital Fairness Act aims to strengthen EU consumer protection in the digital space by banning harmful practices such as dark patterns, addictive design, and misleading influencer marketing. It will complement the GDPR, DSA, and DMA.

- (e) The EU Data Act will create new rules for data access and portability for users of connected devices. Where such data includes personal data, the GDPR and the Data Act will need to be applied in tandem, raising complex compliance questions.
- (f) In the Netherlands, it will be no longer allowed to make telemarketing calls based solely on an existing (ex-)customer relationship as of 1 July 2026. From that date, explicit prior consent (opt-in) will be required for all telemarketing, with limited exceptions (eg, for charities). The ACM has announced stricter supervision in the lead-up to this change.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

See European Union chapter.

12.3 What do you envision the privacy landscape will look like in five years?

The privacy landscape will become increasingly shaped by expanding EU regulation, creating a more complex legal environment where privacy, consumer protection, and AI governance are closely intertwined. Organizations will face growing demands for transparency, accountability, and ethical data use across digital services. Also see question 11.2.

 POLAND 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Poland.

In Poland, the issue of privacy and personal data protection was regulated for the first time by the Constitution of the Republic of Poland of April 2, 1997. In addition, the provisions of the Polish Civil Code on the personal interests of natural persons grant individuals protection with respect to their rights on personal information.

The first comprehensive regulation on privacy was set out in the Act of August 29, 1997 on Personal Data Protection ('PDP'), which implemented the EU Data Protection Directive into the Polish legal system.

The entry into force of the European General Data Protection Regulation ('GDPR') had a great influence on the current Polish data protection regime. The PDP has been repealed and replaced by a new legal framework, implementing and supplementing the GDPR, consisting of:

- (a) the Personal Data Protection Act of May 10, 2018 ('PDPA'), which mainly covers institutional and organizational matters (ie, certification mechanisms, operations of the data protection authority etc); and
- (b) the Act of February 21, 2019 amending certain Acts in connection with the implementation of the GDPR ('Amending Act'), which introduces changes to almost 170 Polish sector-specific regulations, such as those concerning banking or telecommunication law.

These together constitute the universally binding law in the territory of Poland (there are no specific local regulations governing this issue).

The purpose in adopting these new national rules was to adjust the Polish legal system to the requirements set forth by the GDPR, which is directly applicable and remains the most significant legal source of data protection rules in Poland. Therefore, only specific aspects which fall outside the scope of the chapter on the European Union will be discussed below.

1.2 What are the primary laws regulating privacy in Poland? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

As discussed above, the main and primary source of law regulating privacy in Poland is the GDPR. Nevertheless, as the GDPR leaves open clauses for national regulation, the PDPA sets out some derogations from the GDPR. The most relevant are:

- (a) Activities consisting of editing, preparing, creating or publishing press materials and data for the purpose of artistic or literary expression are exempted from certain obligations (eg, to provide privacy notices);
- (b) Controllers conducting public services—if related to the performance of public duties—are exempted from complying with certain obligations (eg, to provide privacy notices and respond to subject access requests);
- (c) The processing of data by entities in the public finance sector is fully exempt if such processing is necessary to perform tasks in the interests of national security; and
- (d) The performance of constitutional and statutory competences of the President of the Republic of Poland, to the extent that this is not covered by national security, is exempted from complying with certain obligations.

Apart from the PDPA, many provisions regulating personal data protection issues are provided for in sector-specific regulations, including the laws regulating marketing activities. These provisions specifically address the issue of consent, which must be collected from subscribers or end users, and which must meet the requirements of data protection law. In Polish law, there is an obligation to obtain permission for, eg, direct marketing by phone or for placing cookies.

In addition, the guidelines issued by the President of the Personal Data Protection Office ('PDPO') may be helpful for a proper understanding of the data protection regulations. There are currently several such guidelines. They refer to many issues related to personal data protection: eg, one describes the regulator's approach to personal data breaches. The guidelines are available in Polish, on the official website of the PDPO.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Please see the European Union chapter.

Although the GDPR and relevant national laws establish binding data protection obligations, self-regulatory initiatives play a complementary role by supporting their practical interpretation and implementation across different sectors. In Poland, two codes of conduct have been officially approved by the PDPO under the GDPR, both within the healthcare sector.

At present, there is no approved code of conduct for the advertising industry in Poland. However, the Polish Interactive Advertising Bureau ('IAB Polska'), one of the key stakeholders in this area, has submitted a code of conduct on good practices for the processing of personal data in the online advertising sector to the PDPO for formal approval according to the GDPR. If approved, it would provide industry stakeholders with a common framework aligned with data protection principles and subject to oversight by an independent monitoring body (accredited for this purpose by the PDPO).

As a side note, it is worth mentioning that, in 2022, the Polish Marketing Association SMB applied for approval of a code of conduct and good practices in the field of personal data protection in direct marketing activities, but its current status is unknown as it is not included in the official PDPO's list.

1.4 How is privacy law enforced in Poland? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The PDPA established a new data protection authority, the PDPO, which has replaced the Inspector General for Personal Data Protection. The main role of the PDPO is to ensure compliance with the GDPR, the PDPA and other data protection laws in Poland.

Apart from the possibility of imposing administrative fines, the PDPO also has the numerous powers listed in the GDPR, such as conducting investigations in the form of data protection audits or issuing warnings and reprimands to the controller or processor in the event of a breach of the GDPR by processing operations. In addition, any assumptions and draft legal acts concerning matters related to personal data protection must be presented to the PDPO for its opinion. Moreover, the PDPO is authorized to request the competent authorities to undertake a legislative initiative or to issue or modify legal acts in matters related to personal data protection.

Importantly, data subjects who have suffered material or non-material damage as a result of a violation of the GDPR are entitled to obtain compensation from the controller or processor. To enforce this right, data subjects may bring civil claims against the liable party. However, such civil claims are still relatively rare in Poland.

Additionally, under Polish law, certain unlawful acts related to the processing of personal data constitute crimes. Committing such crimes may result in a criminal fine, restriction of personal liberty or imprisonment imposed by a court.

As regards approved codes of conduct, their compliance is monitored by bodies accredited by the PDPO. However, it is unclear whether they have taken any enforcement action in this regard, as no information on this matter is publicly available.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Poland?

Please see the European Union chapter.

2.2 Does privacy law in Poland apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Please see the European Union chapter.

The PDPA protects the rights of natural persons with regard to the processing of personal data within the scope specified in the GDPR. There are no other specific national provisions governing this issue.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Poland?

Please see the European Union chapter.

The PDPA does not provide any local derogations from the definitions set out in the GDPR. Therefore, 'personal data' should be understood in accordance with the definition contained in the GDPR.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Please see the European Union chapter.

In addition, Polish regulations on personal data protection contain specific rules on processing of sensitive personal data, for instance:

- (a) authorized representatives of the Supreme Audit Office are entitled to process personal data, except for data revealing political opinions, religious or philosophical beliefs, as well as genetic data and data on addictions, sex life or sexual orientation;
- (b) the Commissioner for Human Rights and the Commissioner for Children's Rights may process sensitive personal data for the purpose of fulfilment of their legal tasks;
- (c) the State Fire Service is permitted to process sensitive personal data in order to recruit its members;

- (d) the Polish National Bank may process, eg, biometric data relating to fingerprints, voice, hands and veins of fingers or hands from providers of services to the Polish National Bank or persons transporting assets with monetary value;
- (e) universities and other academic institutions may process sensitive personal data for scientific purposes, provided that it does not allow for the identification of any data subject; and
- (f) employers are allowed to process employees' biometric data without employees' consent if it is necessary to ensure control over access to particularly important information or to premises requiring special protection.

Apart from the above, processing of personal data for purposes linked to the activities of police and criminal justice authorities must meet the requirements included in the Act of December 14, 2018 on the Protection of Personal Data Processed in connection with the Prevention of and Fight against Crime.

It is also worth pointing out that, in Poland, the PDPO treats the personal identification number ('PESEL number') almost as 'quasi-sensitive' data, even though it is not one of the special categories of data listed in the GDPR. This status becomes especially relevant when assessing personal data breach, as the exposure of a PESEL number significantly increases the risk to the rights and freedoms of individuals and may require notification both to the PDPO and to the data subjects affected.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Please see the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Please see the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Please see the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Please see the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Please see the European Union chapter.

Moreover, pursuant to the Act of October 7, 1999 on the Polish Language, consumers must be informed in Polish. Therefore, any privacy notices addressed to consumers must be in Polish.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Please see the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Please see the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Please see the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Please see the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Please see the European Union chapter.

In Poland, when assessing whether a data protection impact assessment ('DPIA') is required, it is necessary to check the Communication of the PDPO of 17 June 2019, which contains a list of types of personal data processing operations that may require a DPIA (eg, profiling, behavioral analysis, automated decision-making, etc). Generally, a DPIA is required when the planned processing meets at least two of the listed criteria. However, in some cases, a controller may determine that a DPIA is necessary even if only one criterion is met.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Please see the European Union chapter.

Direct marketing in Poland is governed by both the GDPR and the new Electronic Communications Law of July 12, 2024 ('ECL'), which replaced the Telecommunications Law of July 16, 2004, and the Act of July 18, 2002 on the Provision of Electronic Services. The ECL came into force on 10 November 2024.

The ECL requires prior marketing consent to send any commercial information, including direct marketing. When obtaining that consent, all the GDPR requirements apply—ie: it must be freely given, specific, informed, and unambiguous. In practice this means, among other things, that such consent should specify which marketing activities it covers (eg, sending a newsletter) and data subjects must be able to withdraw consent as easily as they gave it. Furthermore, it is clear from the practice of Polish supervisory authorities that separate consent must be collected for each communication channel (eg, email, SMS/MMS, push notifications), as only granular consent meets the GDPR requirement of specificity.

Alongside the marketing consent obtained under the ECL, controllers must comply with the GDPR requirements, including specifying an appropriate legal basis for the processing of personal data for marketing purposes. Depending on the circumstances, this may be legitimate interest, which requires conducting and documenting a legitimate interest assessment ('LIA'), or the data subject's consent. Where consent is selected as the legal basis, it should be obtained separately from the marketing consent.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Please see the European Union chapter.

In Poland, tracking technologies such as cookies, pixels, and SDKs are regulated under the ECL and the GDPR. According to the ECL, prior consent from the user is required for any storage or access to information on their device, unless the technology is strictly necessary for a service the user has expressly requested. Data protection authorities across the EEA require that this consent be 'active'. This means that relying on browser settings is not sufficient; and the GDPR standards for consent, which must be freely given, specific, informed and unambiguous, apply in full.

Before obtaining consent, the controller must provide clear and easily accessible information, specifying, among other things, what types of cookies will be installed, for what purposes, how long they will be stored, and how the user can withdraw consent.

It should be noted that the requirements for cookie banners are also important, especially regarding their visual form. The use of so-called deceptive design patterns is prohibited, such as highlighting the 'Accept all' button with a distinctive color, while making the 'Reject all' option less visible.

7.3 How are loyalty programs and promotions regulated under privacy law?

Please see the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

Please see the European Union chapter.

As there is no influencer-specific privacy law in Poland, the GDPR applies in full. Nonetheless, influencers must comply with the Recommendations of the President of the Office of Competition and Consumer Protection on the Labelling of Advertising Content by Influencers on Social Media, which require paid or sponsored posts to be clearly and legibly tagged. Failure to comply with these Recommendations when running an influencer campaign may be seen as a violation of the GDPR's principles of lawfulness, fairness and transparency, as misleading or hidden advertising can prevent data subjects from receiving clear information about the purposes and parties involved in the processing of their data.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Please see the European Union chapter and question 7.2.

With the customer's permission, a service provider may process other data concerning that customer that are not necessary to provide a given service by electronic means, but are for the purposes of advertising, market research, and customer behavior and preference research, when results of such research serve the purpose of improving the quality of services provided by the service provider.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Please see the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

Please see the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

Please see the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

Please see the European Union chapter.

In Poland, advertising to children and minors under privacy law is governed by a multi-layered legal framework comprising the GDPR, the EU Digital Services Act ('DSA'), and relevant national laws. These regulations impose strict limits on the use of minors' personal data for advertising and restrict the targeting of children with certain commercial content.

The provisions of the GDPR applicable to a child's consent in relation to information society services apply to all processing activities in connection with such offers directly to a child. This encompasses not only the provision of services such as social media platforms, online games, and educational platforms, but also the processing of personal data for ancillary purposes, including personalized advertising, behavioral targeting, and other forms of direct marketing. Therefore, these provisions capture all data processing that is functionally connected to the provision of such services to a minor, even if the advertising or profiling is not the primary feature of the service.

Where consent is relied upon for the processing of personal data in this context, such consent is valid only if the child is at least 16 years old. If the child is under 16, the processing is lawful only if, and to the extent that, consent is given or authorized by the holder of parental responsibility. Poland has not exercised the derogation under the GDPR which allows Member States to set a lower age, so the age of digital consent in Poland remains 16. Controllers must make reasonable efforts to verify, taking into account available technology, that valid parental consent has been obtained where applicable.

The emphasis on consent and verification mechanisms reflects the vulnerability of minors in digital environments and the need to shield them from intrusive data practices, particularly those designed to influence purchasing behavior or exploit behavioral patterns. Controllers must also ensure that privacy notices provided to minors are age-appropriate, intelligible, and transparent.

Although the PDPO has not issued sector-specific guidance on advertising addressed to children, it recognizes the elevated risk involved in the processing of children's data. In its sectoral inspection plan for 2025, the PDPO identified the protection of minors' images as a regulatory priority. In 2024, it published the guidance 'Children's image on the Internet. To publish or not to publish?', addressed to adults, institutions, and organizations, with the aim of encouraging responsible data practices and preventing the misuse of children's images online.

Further obligations stem from the DSA. Providers of online platforms accessible to minors must implement appropriate and proportionate technical and organizational measures to ensure a high level of privacy, safety, and security for child users. Platforms are prohibited from displaying

advertising based on profiling, as defined in the GDPR, when they are aware with reasonable certainty that the user is a minor. However, they are not obliged to process additional personal data solely to determine the user's age.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Please see the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

Please see the European Union chapter.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Please see the European Union chapter.

With regard to the transfer of personal data outside the European Economic Area, the Polish data protection law does not impose any additional requirements, such as notification or reporting obligations to the PDPO.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Please see the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Poland? Are there minimum standards? Does this differ by sector or size of the entity?

Please see the European Union chapter.

9.2 How are personal data breaches regulated in Poland? What are the requirements for notification and response?

Please see the European Union chapter.

The rules regarding personal data breaches in Poland are no different from those set out in the GDPR. In order to notify a personal data breach to the PDPO, it is necessary to use the official data breach-notification form ("form"). The completed form—which must be submitted in Polish—can be filed:

- (a) electronically, by completing the dedicated electronic form available directly on the biznes.gov.pl platform or through electronic inbox on the epuap.gov.pl platform; or
- (b) by traditional mail, sending the hard-copy form to the PDPO's postal address.

It is possible to submit either:

- (i) a complete notification (containing all the required information regarding the personal data breach, including details of how and when the data subjects affected have been—or will be—informed, or a reasoned explanation for not notifying them); or

- (ii) an initial notification (providing basic details, but requiring the submission of a supplementary notification at a later date).

If necessary, a follow-up notification may also be submitted to update or correct the information previously provided.

Importantly, controllers are also required to document all personal data breaches (regardless of whether they require notification), including maintaining a record of personal data breaches.

Moreover, in 2025, the PDPO released an updated guidelines on personal data breaches. The new edition takes into account the latest interpretations of the law, case law and practical guidance to help controllers make the right decisions in the event of a personal data breach. It also includes practical examples and case studies, as well as recommendations on risk assessment and prevention of personal data breaches.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Please see the European Union chapter.

- (a) The PDPA introduced lower financial administrative fines for public authorities. The fines for selected financial sector units, a research institute, and the National Bank of Poland cannot exceed PLN 100,000 (approx €23,400). For other organizations, the limits of the fines are defined in the GDPR.

In addition to administrative liability, the PDPA sets forth criminal provisions and sanctions. Criminal sanctions may be imposed on a given entity for:

- (i) processing personal data, if such processing is not allowed or the processing is carried out without authorization; or
- (ii) obstructing or hindering inspection of personal data processing.

Violation triggers a criminal fine, restriction of personal liberty or imprisonment of up to two years (three years if such processing concerns special categories of data).

Data subjects have the right to lodge a complaint with the PDPO if they consider that the processing of personal data relating to them infringes the GDPR. Moreover, data subjects who have suffered material or non-material damage as a result of a violation of the GDPR are entitled to obtain compensation from the controller or processor. To enforce this right, data subjects may bring a civil claim against the liable party.

- (b) Apart from the consequences described above under the GDPR, the ECL also provides for separate enforcement mechanisms and penalties related to cookies and marketing consents. According to the ECL, non-compliance with legal requirements regarding marketing consents and cookies may potentially result in:

- (i) an administrative fine of up to PLN 1,000,000 (approx €234,000) or 3% of the total turnover for the previous calendar year, whichever is higher (in the case of failing to obtain valid marketing consents); and/or
- (b) an administrative fine of up to 3% of the total turnover for the previous calendar year (in the case of non-compliance with requirements concerning cookies).

Additionally, failure to obtain marketing consent when required may result in the imposition of a criminal fine.

Furthermore, natural persons may raise civil law claims in this regard.

10.2 Do consumers have a private right of action? What remedies are available to them?

Please see the European Union chapter and question 10.1.

Individuals may challenge the violation of their personal data through civil proceedings.

Pursuant to the PDPA, the provisions of the Polish Civil Code apply to claims arising from a violation of the data protection provisions set forth in the GDPR.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The PDPO is becoming increasingly active, although the administrative fines imposed usually remain well below the maximum amount.

The highest administrative fine to date was imposed in 2025, when the PDPO fined Polish Post PLN 27 million (approx €6.3 million) for processing the personal data of 30 million citizens from the PESEL number register without legal basis, in connection with the preparations for so-called ‘envelope parliamentary elections’ in April and May 2020. Previously, for a long time, the highest administrative fine was the one imposed in 2022 on Fortum Marketing and Sales Polska SA in the amount of PLN 4.9 million (approx €1.14 million) for failure to implement appropriate technical and organizational measures to ensure the security of personal data and lack of verification of the processor.

According to the PDPO’s activity report for 2023, a total of 31 administrative fines were imposed that year, totalling PLN 1.23 million (approx €286,840). While this figure is relatively low, it should be noted that a new PDPO took office in 2024 and has appeared (the activity report for 2024 is not yet available) to be more active than their predecessor so far.

For instance, the new PDPO issued a temporary decision on Meta Platforms Ireland Limited, prohibiting the display of false advertisements using the personal data and images of two public figures on Facebook and Instagram within Poland for three months. These decisions were made under provisions in the GDPR, which allow for provisional measures in urgent cases to protect the rights and freedoms of data subjects. The PDPO considered the unauthorized use of personal data and deepfake content to be serious violations affecting the dignity, privacy, and security of the individuals involved.

Additionally, the PDPO imposed an administrative fine of PLN 314,302 (approx €73,296) on Toyota Bank Polska SA for failing to include the profiling of clients and potential clients for creditworthiness assessment in its record of processing activities and for not conducting a data protection impact assessment (‘DPIA’) related to that profiling. Although profiling was carried out to assess the creditworthiness of clients (and not for marketing purposes), the case highlights the importance of properly documenting all high-risk processing operations and conducting a thorough risk analysis in line with the GDPR requirements.

One of the most important recent judgments was one that the Voivodship Administrative Court in Warsaw rendered in 2024. The court confirmed that customer satisfaction surveys, displaying offers in a mobile application, and sending text messages informing about the functionality of a mobile application constitute marketing activities if they influence customer decisions, and their legality requires the prior, explicit consent of the customer to marketing activities.

As for civil claims—although data subjects may seek compensation for material or non-material damage under the GDPR, such actions remain relatively rare in Poland in practice.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Poland?

Cultural considerations have a significant influence on the interpretation and enforcement of privacy laws in Poland, particularly in the fields of marketing and advertising. One of the most prominent factors is the societal distrust toward surveillance and intrusive data collection, shaped by Poland's historical experience with authoritarian regimes. This legacy of state control over private life contributes to heightened public sensitivity to privacy violations. The scale of this cultural factor is evidenced by the number of complaints lodged with the PDPO. According to the PDPO's activity report for 2023, the PDPO received 6,962 complaints, including 2,659 directed against private sector entities. This reflects a consistently high level of public engagement with data protection enforcement.

Public awareness of privacy rights is steadily growing, and media outlets often highlight privacy-related controversies, particularly when they involve large platforms or foreign companies. As a result, enforcement decisions may be influenced not only by legal violations but also by the visibility of the case and its potential impact on public trust.

Taken together, these cultural considerations underscore the importance of aligning data-driven marketing and advertising practices with the expectations of Polish society. Organizations operating in Poland should not rely solely on a formalistic reading of the GDPR but also assess how their practices are likely to be perceived in light of evolving public attitudes toward privacy and digital fairness.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Several regulatory developments are currently reshaping the privacy and digital compliance landscape in Poland, and companies operating in this jurisdiction should closely monitor these evolving areas:

- (a) One key area is the anticipated update to the PDPO guidance on data processing in the employment context. Announced in 2024, this long-awaited update—still in development following a public consultation—will likely influence how the PDPO interprets the GDPR in conjunction with Polish employment law. New interpretations may emerge regarding the lawful bases for processing employee data, retaining data of rejected job applicants, monitoring practices, and the roles of trade unions or employee representatives.
- (b) Another significant development is the PDPO's revised guidelines on personal data breaches, published in February 2025. The new guidelines take a more restrictive approach to when a personal data breach can be considered unlikely to pose a risk to individuals' rights and freedoms, encouraging the notification of doubtful cases and strengthening the role of the PDPO in incident management. The updated interpretation is expected to influence internal policies, response timelines, and the assessment methodologies adopted by controllers and processors.
- (c) Artificial intelligence regulation is also gaining prominence. In late 2024, Poland presented a Draft Act on Artificial Intelligence Systems to create a regulatory and institutional environment for the application and enforcing the EU AI Act. The proposed law establishes a dedicated national supervisory body and outlines procedures for registration, conformity assessment, and the establishment of regulatory sandboxes.

In addition to the forthcoming regime on enforcing the AI Act, the GDPR already applies to AI systems that process personal data. This includes profiling, segmentation, and content generation, where principles such as purpose limitation, data minimization, and transparency remain crucial. The PDPO has already joined EU-level scrutiny of generative AI systems, such as ChatGPT, signalling that AI innovation will be held to existing privacy standards even before the AI Act takes effect.

- (d) Finally, businesses should monitor legislative initiatives aimed at protecting minors from harmful online content. A draft Act published in early 2025 introduces risk analysis and mandatory age verification for providers of adult content, along with a centralized register of non-compliant domains. The proposal also includes safeguards to prevent unlawful expansion of data processing and limits the use of age verification data. If adopted, it will apply broadly to digital service providers offering access to content in Poland, reinforcing the growing overlap between content regulation and data protection law.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The PDPO is known for its pragmatic but conservative approach to enforcement. In practice, companies operating in Poland should be prepared not only to demonstrate the legal basis for their processing operations but also to clearly articulate the rationale behind those operations and how they align with data protection principles. Maintaining up-to-date documentation, conducting regular risk assessments, and embedding data protection by design and by default into business processes remain key components of a robust compliance strategy.

Since 2022, the PDPO has intensified enforcement, including issuing administrative fines for lack of cooperation—particularly where entities fail to respond to requests or ignore official correspondence. For controllers and processors, this signals that cooperation with the PDPO is not optional but a core compliance duty under the GDPR. The PDPO views non-cooperation as a serious violation and has demonstrated a willingness to use its full range of enforcement powers.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Please see the European Union chapter. In addition, changes in the privacy landscape in Poland are described above, so please see questions 1.3, 7.1, 7.2, 7.4, 7.9, 9.2, 10.1, 10.3, 11.2, and 11.3.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

One of the key challenges for companies operating across the European Union is managing the fragmented implementation of the GDPR. Although the GDPR aims to achieve harmonization, national laws—particularly in areas such as employment and health data—often introduce diverging requirements, making cross-border compliance both complex and costly. This fragmentation is further exacerbated by varying interpretations among data protection authorities of fundamental GDPR concepts, such as ‘legitimate interest’ or ‘disproportionate effort’, creating enforcement risks even for companies acting in good faith.

Meanwhile, the regulatory landscape continues to evolve rapidly, with new legislation such as the Data Act and the AI Act reshaping compliance expectations. In this dynamic environment, rigid, box-ticking approaches are no longer sufficient. Instead, companies must develop adaptive, principle-based compliance strategies and privacy programs that can accommodate national differences while remaining resilient to legal and technological changes.

12.3 What do you envision the privacy landscape will look like in five years?

On May 21, 2025, the European Commission published a proposal to amend the GDPR as part of its Omnibus IV Simplification Package ('Proposal'), which aims to reduce the compliance burdens for small and medium-sized enterprises ('SMEs') and the newly defined category of small mid-caps ('SMCs'). The Proposal's key change is an extension of the record-keeping exemption under the GDPR to organizations with fewer than 750 employees, regardless of whether processing is occasional. However, this exemption would not apply where the processing is likely to result in high risks to data subjects' rights and freedoms, or involves special categories of data, meaning many SMEs and SMCs may still need to maintain records of processing activities. The Proposal also requires that the needs of SMEs be considered when developing codes of conduct and certification mechanisms. The legislative process is ongoing, with adoption expected no earlier than 2026.

Regardless of these planned amendments, the privacy landscape in the EU over the next five years will be characterized by an increasingly complex and multi-layered regulatory environment, with the GDPR being just one piece of a broader data governance puzzle. New sectoral regimes—such as the AI Act, the Data Act, and a growing number of European data spaces—will reshape the way organizations collect, share, and process data in various fields. It seems that one of the most important and emerging challenges will be the protection of mental privacy—the individual's right to keep their thoughts, emotions, and cognitive processes free from unauthorized access or manipulation. Neurodata, including signals from the brain or nervous system and inferences about emotional states or preferences, will require enhanced safeguards as regulators begin to treat such data with the same sensitivity as data concerning health or biometric data. As data spaces expand beyond the European Health Data Space into areas such as energy, finance, and mobility, companies will face increasing inter-operability obligations and governance requirements that extend far beyond traditional compliance. Divergences in the interpretation of the GDPR and other EU digital laws which influence privacy, by data protection authorities and other relevant supervisory authorities, will continue to pose a challenge, especially for cross-border operations, making the ability to anticipate and adapt to regulatory changes essential. In this environment, successful organizations will move beyond reactive compliance and invest in proactive privacy by design strategies that embed ethical data use and regulatory flexibility.

 PORTUGAL

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Portugal.

Privacy is regulated by statutory law, such as constitutional rights, national law and European law. The main legal source for data privacy protection is the European General Data Protection Regulation ('GDPR'). At a national level, the Portuguese Parliament approved Law No 58/2019, of 8 August ('GDPR Implementation Law'), which ensures the implementation of the GDPR in Portugal, which regulates privacy alongside multiple sector-specific stipulations contained in other legislation (see question 1.2).

All this legislation is interpreted and enforced by the Portuguese data protection authority ('DPA') which is an independent body, with powers of authority throughout national territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law. The Portuguese DPA issues its own guidelines and deliberations, which may be taken into account as a best-practice basis and could be used by the administrative courts when assessing decisions and/or administrative offence proceedings related to data protection matters. In addition to the guidelines issued by the Portuguese DPA, the guidelines issued by the European Data Protection Board may also be used by legal and judicial operators when dealing with privacy matters.

1.2 What are the primary laws regulating privacy in Portugal? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The main legal source for data privacy protection is the GDPR.

At a national level, the GDPR Implementation Law establishes specific requirements applicable to, inter alia:

- (a) employment relationships;
- (b) a child's consent;
- (c) personal data of deceased persons;
- (d) portability and inter-operability/interconnection of data;
- (e) video surveillance;
- (f) rules applicable to data protection officers; and
- (g) health and genetic data.

However, please note that the Portuguese DPA issued Deliberation No 2019/494 on 3 September, according to which it states that it will not apply certain articles of the GDPR Implementation Law, because it considers that the Law violates the rule of law of the European Union and compromises the effectiveness of GDPR dispositions.

With respect to marketing aspects, the relevant stipulations from a data protection point of view are contained in the GDPR and in the E-Privacy Law (Law No 4172004 of August 18). The legal framework applicable to unfair commercial practices also regulates certain aspects of marketing activities.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Portugal does not have any self-regulatory bodies which enforce privacy law.

The data protection legislation is enforced by the Portuguese DPA, which carries out the tasks specified in the GDPR.

ARP (the Portuguese advertising self-regulator) has not issued any decisions regarding advertisers' misusing or misprocessing personal data.

1.4 How is privacy law enforced in Portugal? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Portugal does not have any self-regulatory bodies which enforce privacy law.

The data protection legislation is enforced by the Portuguese DPA, which carries out the tasks specified in the GDPR, as well as:

- (a) gives its non-binding opinion on legislative and regulatory measures related to data protection, as well as on legal instruments in discussion with European and international institutions;
- (b) monitors compliance with GDPR dispositions and further legal and regulatory dispositions related to personal data protection, rights, freedoms and guarantees of data subjects, and remedies and sanctions non-compliance;
- (c) makes available a list of data processing activities subject to a data protection impact assessment;
- (d) prepares and submits, to the European Committee for Data Protection, the criteria projects for the accreditation bodies for the monitoring of codes of conduct and certification bodies; and
- (e) co-operates with the Portuguese Institute for Accreditation.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Portugal?

Regarding the criteria that establishes the applicability of the GDPR to companies, please see the European Union chapter.

The GDPR Implementation Law renders companies subject to its content based on, alternatively, a territorial and an extraterritorial connection. Specifically, the Law applies to companies carrying out personal data processing activities inside and outside the national territory when the processing:

- (a) it is carried out in the context of the activity of an establishment located in the national territory;
- (b) it affects data subjects who are in the national territory, when the processing activities are subject to the provisions of the GDPR (see the European Union chapter question 2.2(b)); or
- (c) it affects data registered at consular posts of Portuguese nationals residing abroad.

However, the DPA has decided that it will not apply these provisions in future cases, as it considers that such rules violate GDPR dispositions.

The GDPR Implementation Law does not apply to personal data files created and maintained under the responsibility of the Portuguese Republic's System of Information.

2.2 Does privacy law in Portugal apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

For the general requirements for foreign companies, see the European Union chapter. Please also see question 2.1.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Portugal?

For the definition of ‘personal data’ applicable in the Portuguese jurisdiction, please see the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

In addition to the classification (and subsequent obligations) contained in the GDPR, the GDPR Implementation Law establishes specific requirements related to processing of certain special categories of personal data. We highlight the following:

- (a) **Child’s consent:** The personal data of a child may only be processed if based on consent and, in relation to the offer of information society services directly to the child, if the child is at least 13 years old. Where the child is below 13 years old, such processing is lawful only if consent is given by someone with parental responsibility for the child, preferably using secure authentication.
- (b) **Personal data of deceased persons:** A deceased person’s rights provided for in the GDPR, namely the right of access, rectification and erasure, may be exercised by the person designated by the deceased person or, failing that, by the deceased person’s heirs. Data subjects may instead determine that no-one may exercise such rights after their death.
- (c) **Health and genetic data:** Access to health and genetic data is governed by the ‘need to know’ principle, and the data controller is obliged to notify the data subject of any access to such personal data, which means that the controller will, necessarily, have to implement a traceability and notification mechanism. A duty of confidentiality is imposed on persons who have access to health data.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

For norms concerning the processing of anonymized, pseudonymized, or de-identified data processing, please see the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

For the key obligations for companies under privacy laws, please see the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

In addition, the Portuguese GDPR Implementation Law exceptionally allows:

- (a) the processing of personal data by public authorities for purposes other than those determined at the moment of data collection. The purpose for the processing activity must be the pursuit of a public interest that cannot otherwise be served; and
- (b) the transmission of personal data between public authorities for purposes other than those determined at the moment of data collection. The processing shall be the subject of a protocol establishing the responsibilities of each intervening entity, both in the act of transmission and in other processing to be carried out.

However, the Portuguese Data Protection Authority has decided that it will not apply these exceptions, because it considers that they violate the GDPR.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes—Portuguese privacy laws always require a lawful basis for processing personal data.

For the lawful basis for processing personal data please see the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

For the information that companies must include in their privacy notices please see the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

For the privacy rights consumers have concerning their personal data in advertising contexts see the European Union chapter.

In addition to the rights established by Union law, the Portuguese GDPR Implementation Law stipulates:

- (a) data subject rights belonging to the deceased may be exercised by their lawful heirs; and
- (b) data portability only covers data provided by the data subject.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

For the general circumstances in which companies must obtain consent or provide opt-out options for advertising, please see the European Union chapter.

For the details on the requirements and limitations to direct marketing, please see question 7.1.

Indirect marketing does not impose specific requirements beyond those mentioned in the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

For the data protection relationships that may be established between a company and its vendors or other third parties hired in connection with advertising, please see the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

For the data protection obligations that must be fulfilled in a contract between a company and its vendors or other third parties hired in connection with advertising, please see the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

For the due diligence measure that must be adopted by companies and for the requirements to undertake a data protection impact assessment, for the purpose of data protection, please see the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

In addition to the regulation referred to in the European Union chapter, direct marketing is regulated by Portuguese E-Privacy Law.

The Portuguese E-Privacy Law stipulates that controllers are sometimes required to obtain the data subject's prior consent, and also stipulates times when they are required to offer data subjects the possibility to opt of the contact listing based on: the type of product/service offered, the means of communication used, and the existence of prior business relationship.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

For the general regulation of tracking technologies, please see the European Union chapter.

With regard to cookies, the E-Privacy Law establishes that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed where the subscriber or user concerned has given prior consent, having been provided with clear and comprehensive information in accordance with the data protection regulations, inter alia, about the purposes of the processing.

We note that, pursuant to the GDPR, consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to them. Therefore, silence, pre-ticked boxes or inactivity cannot constitute consent.

Notwithstanding, this does not apply to technical storage or access which is strictly necessary in order for the provider of an information society service to provide a service which has been explicitly requested by the subscriber or user.

The E-Privacy Law also provides for specific requirements applicable to traffic data.

In 2021, the Portuguese DPA announced the preparation of Cookie use-specific Guidelines. However, those Guidelines have not yet been issued.

7.3 How are loyalty programs and promotions regulated under privacy law?

For the regulation of loyalty programs and promotions see the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

The Portuguese GDPR Implementation Law establishes that the protection of personal data must not affect the freedom of speech, of information and of the press, including data processing for journalistic, academic, artistic and literary purposes. Notwithstanding, freedom of speech does not legitimize the disclosure of personal data, such as addresses and contacts, except those in common knowledge.

General influencer marketing has been object of some self-regulation, but only some specific products (milk substitutes for infants being one example) have had their advertising by digital influencers externally regulated.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

For the regulation of targeted advertising see the European Union chapter.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

For the regulation of the digital identity resolution and clean room technologies please see the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

For the regulation of location-based advertising please see the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

For the regulation of data brokers please see the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

For the general regulation of advertising to children and minors, please see the European Union chapter.

In addition to the obligations contained in the GDPR, the GDPR Implementation Law establishes specific requirements related to processing of children's personal data. See question 3.2(a).

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

For the general regulation of profiling or the use of AI or automated decision-making please see the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

There are no other relevant regulations concerning the processing of personal data in the context of advertising.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

For general restrictions on the transferring of personal data, please see the European Union chapter.

Pursuant to the Portuguese GDPR Implementation Law, transfers of personal data to countries outside the European Union/third countries or to international organizations, carried out in compliance with legal obligations by public entities within their authority powers, are considered of public interest (see European Union chapter question 8.1(c)).

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

For additional considerations on personal data transfers, please see the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Portugal? Are there minimum standards? Does this differ by sector or size of the entity?

For data security regulations please see the European Union chapter.

Lastly, we highlight that the Portuguese DPA has issued Guidelines on the organizational and safety measures that must be adopted by controllers and processors of personal data.

9.2 How are personal data breaches regulated in Portugal? What are the requirements for notification and response?

For breach management regulations please see the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

In addition to the provisions regulating penalties for non-compliance mentioned in the European Union chapter, note that:

- (a) The Portuguese GDPR Implementation Law provides for administrative offences in addition to those provided for in the GDPR. However, the Portuguese DPA has decided that it will not apply some of these in future cases, due to the fact that it has considered that they violate the GDPR.
- (b) The minimum and maximum limits on fines for very serious and serious administrative offences vary according to the type of infringer (large company, small and medium-sized company or natural person).

- (c) The DPA has established the possibility of waiving the application of fines for a period of three years as from the entry into force of the law, upon a reasoned request made by public entities addressed to the DPA. The legal provision of this prerogative shall be subject to re-evaluation three years after August 9, 2019.
- (d) The GDPR Implementation Law specifies several crimes with regard to personal data, such as:
 - (i) the use of data incompatible with the purpose of the collection;
 - (ii) improper access;
 - (iii) data diversion;
 - (iv) data corruption or destruction;
 - (v) insertion of false data;
 - (vi) breach of the duty of confidentiality; and
 - (vii) failure to comply with obligations under the GDPR or the GDPR Implementation Law.

The penalties, as well as the types of crimes, are similar to those previously provided for in Law No 67/98 of 26 October (the former Portuguese Data Protection Law), except that the maximum penalty in respect of the crime of violation of the duty of professional confidentiality has been reduced by half.

Attempting to commit such crimes is also always punishable.

10.2 Do consumers have a private right of action? What remedies are available to them?

For consumers private right of action and corresponding remedies please see the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Neither the ARP (advertising self-regulator), the Portuguese DPA or the General Directorship for Consumers (advertising supervisory entity) have brought any claims or proceedings concerning alleged privacy non-compliance involving advertising.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Portugal?

None.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

For the hot topics and anticipated legal challenges see the European Union chapter.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Portuguese DPA has started to bring administrative offense proceedings; in particular it imposed:

- (a) a fine of €400,000 on a hospital for three violations of the GDPR, namely:
 - (i) violation of the processing basic principles;
 - (ii) violation of the integrity and confidentiality of personal data; and
 - (iii) failure to implement technical and organizational measures to ensure a level of security adequate to the risk of the processing;

- (b) a fine of €107,000 on a consumer protection association for sending unsolicited emails for direct marketing or advertising purposes without obtaining prior consent (in violation of the GDPR and the E-Privacy Law);
- (c) a fine of €20,000 on a car brand for denial of the right of access to recorded phone calls by the data subject; and
- (d) a fine of €1,250,000 on the City Council of Lisbon (the fine amended, on appeal to the Court of Appeal, to €1,027,000), in the context of the case known as ‘Russiagate’, for having disclosed personal data of protesters to embassies of several countries.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

For the most significant changes in the privacy landscape since 2022 please see the European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies and judicial and legal operators may experience uncertainties due to the decision of the DPA, which has chosen not to enforce several provisions of the Portuguese GDPR Implementation Law (refer to question 1.2). This decision has yet to be reviewed or clarified by the Portuguese courts.

12.3 What do you envision the privacy landscape will look like in five years?

The Portuguese DPA has been more active in the enforcement of fines; it is possible that we will continue to see an increase in its control and effective enforcement of fines under the data protection legislation, as well as it carrying out random audits to check compliance with data protection law on a more frequent basis, and audits initiated by individual complaints.

Additionally, we also envisage an increase in claims from a data protection law and consumer protection law perspective.

ROMANIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Romania.

In Romania, privacy is regulated by statutory law, with the right to privacy being recognized as a constitutional right. Moreover, the right to privacy is reinforced by the Romanian Civil Code and several specific laws, which transpose and apply relevant EU provisions, including the GDPR.

Ensuring the right to privacy for its citizens has been a constant concern for Romanian authorities, which have adopted a rigorous legal framework and institutional mechanisms for enforcement.

The Romanian Constitution states that: ‘The public authorities are bound to respect and protect intimate, family and private life.’

The Romanian Civil Code, adopted by Law No 287/2009, also provides for the protection of privacy, with provisions regulating non-patrimonial personal rights, setting out:

- (a) the right of every person to respect for their dignity and private life;
- (b) protected personal attributes, including name, image, voice, and private correspondence;
- (c) actions considered infringements on private life; and
- (d) the processing of personal data.

The Romanian Supreme Court has also paid great attention to aspects related to data privacy, stating, in a well-known decision, that ‘surname and forename are considered personal data, whether or not there is enough to identify the persons. In the requirements of free access to information of public interest, when the information of public interest and information representing personal data are comprised in the same document, the public interest information may be accessed solely by anonymizing personal data.’

Currently, the open clauses of the GDPR are implemented in Romania through Law No 190/2018 on GDPR implementing measures (‘Privacy Law’). In addition, Law No 129/2018 for amending and supplementing Law No 102/2005 regarding the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing (‘Law 129/2018’) aligns the Romanian supervisory authority’s powers with the GDPR.

Focusing on advertising, Law No 506/2004 regarding personal data processing and the protection of private life in the electronic communication sector (‘Law 506/2004’) implements the ePrivacy Directive and regulates communications sent through the public electronic communication networks and through the electronic communication services, and provides certain requirements that need to be complied with when sending electronic communications to data subjects.

1.2 What are the primary laws regulating privacy in Romania? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) As for all the EU states, in Romania, the GDPR represents the fundamental source for ensuring the implementation of data protection rights, as well as all the relevant aspects concerning data privacy.
- (b) The main provisions established by the Privacy Law, when implementing the open clauses of GDPR concern the following aspects:

- (i) defining the national identification number as the number with which an individual is identified in public records, such as personal identification number, the series and number of the identity document, passport number and number of driving license or the number of social health insurance;
 - (ii) how public authorities are treated in comparison to private operators with respect to enforcing data protection provisions;
 - (iii) data processing at work; and
 - (iv) that the processing of genetic data, biometric data and health data is permitted solely with the explicit consent of the data subject or if processing is based on a legal provision.
- (c) Focusing on the advertising aspect of data privacy, Law No 506/2004 regulates the communications sent through public electronic communication networks and through electronic communication services, stating that a natural person should receive electronic communications (or any other type of communications) only upon granting consent.
- (d) Additional provisions on commercial communications are regulated by Law No 365/2002 regarding electronic commerce ('Law 365/2002'), that alongside the GDPR, establishes that sending electronic communications is forbidden if a natural person did not give prior consent.
- (e) Law No 363/2018 on the protection of individuals regarding the processing of personal data by competent authorities implements the Law Enforcement Directive (2016/680/EU) and governs the processing of personal data by competent authorities for law enforcement purposes.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In Romania, self-regulation complements formal privacy legislation by establishing voluntary standards for responsible data use in advertising. The Romanian Advertising Council ('RAC'), the principal self-regulatory body, issues a Code of Best Practices in Commercial Communication that aligns with data protection principles such as fairness, transparency, and consent. Although the RAC does not enforce privacy law per se, its guidelines discourage intrusive marketing tactics and the misuse of personal data, particularly in targeting vulnerable consumers or sending unsolicited communications.

Self-regulation promotes a culture of compliance, educates advertisers on privacy-sensitive practices, and helps preempt legal violations by encouraging ethical behavior. It plays a practical role in filling gaps where statutory rules may not provide detailed guidance, especially in emerging digital marketing techniques. However, adherence to self-regulation is voluntary, and it lacks legal enforcement power.

1.4 How is privacy law enforced in Romania? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy law in Romania is primarily enforced through statutory mechanisms under the supervision of the National Supervisory Authority for Personal Data Processing ('ANSPDCP'), which is the national data protection authority. The ANSPDCP is responsible for monitoring compliance with the GDPR, Law No 190/2018, and other relevant legal provisions. Its enforcement powers include conducting investigations, issuing warnings and corrective orders, and imposing administrative fines that can reach up to €20 million or 4% of global turnover, in line with the GDPR.

As it is a European objective to encourage the establishment of certification mechanisms which would allow data controllers and data processors to demonstrate that their processing operations comply with the GDPR, in 2021, the ANSPDCP issued Decision No 20/2021 which sets out the necessary requirements to allow the accreditation of certification bodies, and considers general requirements regarding accreditation, structure and process, resources, the management system and other additional requirements, including those related to the European standard ENISO/IEC 17065/2012.

In addition to regulatory enforcement, data subjects may pursue private actions under civil law, especially under the Romanian Civil Code, seeking remedies such as cessation of unlawful processing and compensation for damages.

While self-regulatory bodies like the RAC provide guidance and ethical oversight in the advertising sector, their enforcement capacity is limited to reputational mechanisms, such as public criticism or exclusion from membership. They do not impose legal penalties, but may influence compliance through peer pressure and voluntary commitments.

Enforcement may also involve sectoral authorities, such as the Financial Supervisory Authority or the National Authority for Management and Regulation in Communications, in cases involving financial or telecommunications data processing, respectively.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Romania?

- (a) A company becomes subject to Romanian privacy laws under the following conditions:
 - (i) **Establishment in Romania:** If a company has a physical presence, such as an office, branch, or subsidiary in Romania, and processes personal data in the context of its activities, it falls within the scope of the GDPR and national data protection laws.
 - (ii) **Targeting individuals in Romania:** Even without a physical presence, a company established outside the European Union that offers goods or services to individuals in Romania or monitors their behavior (eg, through online tracking) is subject to the GDPR.

Both data controllers (entities that determine the purposes and means of processing personal data) and data processors (entities that process data on behalf of controllers) are subject to privacy laws in Romania. This includes both public and private entities.

- (b) While public authorities are subject to the same data protection principles, Law No 190/2018 provides certain procedural distinctions:
 - (i) **Remediation period:** Upon identifying a data protection infringement by a public authority, the ANSPDCP issues a warning accompanied by a remediation plan. The public authority is granted a period of up to 90 days to address the identified issues before any fines are imposed.
 - (ii) **Capped fines:** If the public authority fails to implement the remediation measures within the stipulated period, ANSPDCP may impose fines. However, these fines are capped at RON 200,000 (approx €39,000), which is significantly lower than the maximum fines applicable to private entities under the GDPR.

2.2 Does privacy law in Romania apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. Given that the Privacy Law implements the open clauses of the GDPR, its provisions apply whenever the GDPR is applicable. Therefore, the Romanian Privacy Law is applicable to companies outside Romania that process personal data in Romania or transfer data to those countries that fall within the scope of the GDPR.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Romania?

The Romanian legal provisions have not defined ‘personal data’, given that it is already defined in the GDPR.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

Furthermore, the Romanian Privacy Law establishes that processing of genetic data, biometric data and health data is permitted solely with the explicit consent of the data subject or where processing is based on a legal provision.

Moreover, the Privacy Law provides that, when special categories of personal data are processed based on public interest, the controller must take the following safeguards:

- (a) implement adequate technical and organizational measures for fulfilling the principles of the GDPR, especially data minimization, data integrity and confidentiality;
- (b) appoint a data protection officer, when necessary; and
- (c) establish storage periods based on the nature and purpose of processing, as well as specific periods after which personal data must be erased or revised for erasure.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under Romanian privacy law, the treatment of anonymized, pseudonymized, or de-identified data fully aligns with the provisions of the GDPR.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Romanian privacy law aligns with the GDPR. See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under Romanian privacy law, companies must provide clear, accessible, and complete information in their privacy notices when processing personal data for advertising purposes. See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Please see the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

In Romania, companies must obtain prior consent before sending unsolicited commercial communications such as emails, SMS messages, or automated calls, in accordance with Law No 506/2004 (which transposed the ePrivacy Directive). Consent must be freely given, specific, informed, and expressed through a clear affirmative action. It is also required for the use of cookies that are not strictly necessary, and for processing special categories of personal data for advertising purposes.

Opt-out is permitted only in limited situations. This applies when the company has obtained the individual's contact details during the sale of a product or service and uses them to promote similar offerings. In such cases, the individual must be clearly informed and given the opportunity to refuse the use of their data both at the time of collection and in each communication.

Marketing messages must be clearly identified and must contain a visible and simple unsubscribe mechanism. Companies must also maintain records of consent and respect any withdrawal or objection without delay.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Please see the European Union Chapter.

Romanian privacy law requires that companies engaging vendors or third parties for advertising purposes ensure those parties process personal data lawfully and under appropriate contractual safeguards.

When an advertising vendor (such as an agency, DSP, SSP, or data provider) processes personal data on behalf of the company, a written data processing agreement is required. This agreement must define the scope, purpose, and limits of processing and include obligations on confidentiality, security, sub-processing, and cooperation with the controller.

If the third party acts as a joint controller (eg, when jointly determining the purpose of data-driven advertising), both parties must clearly allocate responsibilities and inform individuals of the arrangement.

Controllers must also carry out due diligence to ensure vendors implement adequate technical and organizational measures. Where international transfers occur, appropriate safeguards such as standard contractual clauses must be in place.

In short, companies must treat advertising-related third parties as processors or controllers and remain accountable for ensuring GDPR-compliant data processing throughout the chain.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Please see the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Please see the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter.

Direct marketing in Romania is primarily regulated by Law No 506/2004 and Law No 365/2002. As a general rule, Law No 506/2004 prohibits sending unsolicited commercial communications via electronic means (such as email, SMS, or automated systems) without the prior express consent of the recipient.

However, there is a limited exception: if a natural or legal person obtains the recipient's email address directly during the sale of a product or service, they may use it for marketing similar products or services, provided that the recipient is offered a clear and free opportunity to object, both at the time of collection and in each subsequent communication. This is commonly referred to as the 'soft opt-in' rule.

All direct marketing messages must clearly identify the sender and include an easy and accessible opt-out mechanism. The GDPR also applies, particularly when personal data is used for targeting or profiling in the context of direct marketing.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Please see the European Union chapter.

7.3 How are loyalty programs and promotions regulated under privacy law?

Please see the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

Please see the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

In Romania, targeted advertising, including behavioral and personalized advertising, is regulated by the GDPR and Law No 506/2004. These activities usually involve the processing of personal data, such as tracking user activity across websites or profiling individuals for advertising purposes. As such, they typically require the explicit, informed, and freely given consent of the data subject prior to processing.

In addition, data subjects must be clearly informed when profiling is used for advertising. The privacy notice must explain the purpose of the profiling, the underlying logic, and the potential consequences for the individual. If such profiling is performed on a large scale or involves special categories of data, a data protection impact assessment is not only recommended but also mandatory.

By contrast, contextual advertising, which serves ads based on the content of the webpage rather than user behavior or identity, generally does not involve personal data processing. As such, it does not trigger the same obligations under the GDPR or Law No 506/2004 and can typically be carried out without consent.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

In addition to the GDPR (for which see the European Union chapter), Romanian law (specifically Law No 506/2004) applies to digital identity resolution and clean room technologies when these involve access to a user's terminal equipment, use of electronic communications services, or processing of traffic and location data.

If the technology relies on cookies, fingerprinting, or similar device-level identifiers, prior user consent is required, and the user must be provided with clear and complete information before giving that consent. This applies even when such technologies are embedded in clean rooms or identity resolution mechanisms. Exceptions to the consent rule apply only in very limited cases, such as when the operation is strictly necessary for communication, or a service explicitly requested by the user.

When these tools process traffic data (such as metadata related to communications) or location data, additional rules apply. Express prior consent from the user is required before such data may be processed for marketing, analytics, or identity resolution purposes. These provisions remain applicable even if the data is collected by a third-party vendor acting on behalf of the controller.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

Additionally, Law No 506/2004 specifically regulates the use of location data other than traffic data collected through electronic communication services. Such data may only be processed for value-added services (such as location-based advertising) if the user has given explicit prior consent. The user must be clearly informed in advance about the types of location data processed, the purpose and duration of processing, and any potential disclosure to third parties. Additionally, users must be provided with a simple and free mechanism to withdraw their consent or to temporarily refuse processing for each session.

7.8 How are data brokers defined and regulated under privacy law?

Please see the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

Please see the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Please see the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

Law No 158/2008 prohibits advertising that deceives or is likely to deceive consumers, including by omission of essential data. This may overlap with privacy rights if the ad implies personal targeting or misuses personal data to suggest individual customization.

Law No 363/2007 implements the EU Unfair Commercial Practices Directive and prohibits aggressive or misleading advertising tactics, especially toward vulnerable consumers. This is relevant when profiling or targeting minors or the elderly based on inferred characteristics.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Please see the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Please see the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Romania? Are there minimum standards? Does this differ by sector or size of the entity?

The GDPR imposes the general framework regarding the standard required in ensuring the security of personal data. Thus, please see the European Union chapter.

In addition, companies, as well as public authorities and bodies, have, as an instrument in implementing the adequate security standard, a consultation procedure with the ANSPDCP. These entities can file a formal letter to the national supervisory authority with respect to a certain type of processing, requiring advice in order to ascertain the proper method of establishing the security of personal data.

Also please note that Romanian law does not formally distinguish data security requirements based on the sector or the size of the entity.

9.2 How are personal data breaches regulated in Romania? What are the requirements for notification and response?

For most data controllers, breach notification obligations are governed by the GDPR, complemented by Law No 190/2018, which confirms the authority of the ANSPDCP to receive and process notifications. Notifications must be submitted within 72 hours of becoming aware of the breach, using the procedure and online forms provided on the ANSPDCP website. Although a phone call is not required, the notification must be digitally signed with a qualified electronic signature, otherwise it will not be considered valid. In some cases, the ANSPDCP may request supporting documentation in physical format.

For providers of public communications networks or services, Law No 506/2004 and ANSPDCP Decision No 184/2014 (which implements Commission Regulation 611/2013/EU) outlines a distinct reporting obligation. These providers must notify both the ANSPDCP and, in some cases, affected subscribers of security breaches concerning personal data. The notification must be submitted using a standardized form via the dedicated digital platform hosted by ANSPDCP. Personal data breaches must be notified in all situations, regardless of whether they are likely to pose risks to data subjects.

In both cases, failure to notify a data breach, or delays in notification, may trigger investigations and sanctions by the authority.

In terms of response, controllers are required to document the breach, assess the risk to individuals, mitigate its effects, and notify affected data subjects if there is a high risk to their rights and freedoms. They must also take appropriate corrective measures to prevent recurrence and provide the ANSPDCP with supporting documentation upon request.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

Moreover:

- (a) For private entities, non-compliance with the GDPR or with Law No 190/2018 constitutes a contravention and is sanctioned accordingly. Sanctions may include a warning or administrative fine.
- (b) For public authorities and bodies, Law No 190/2018 provides a distinct enforcement mechanism. The authority first issues a warning and a remediation plan. If the public entity fails to implement the remediation measures, the ANSPDCP may impose a fine. Fines are capped as follows:
 - (i) for contraventions: between 10,000 and 100,000 RON (approx €2,000–20,000).
 - (ii) for more serious breaches (eg, in cases involving violations of fundamental GDPR principles such as lawful processing, data subject rights), or failure to comply with ANSPDCP decisions): between 10,000 and 200,000 RON (approx €2,000–40,000).

In all cases, the ANSPDCP may also apply corrective measures under the GDPR, such as orders to suspend processing or bring it into compliance.

10.2 Do consumers have a private right of action? What remedies are available to them?

Please see the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The ANSPDCP actively enforces data protection laws (as of this year, the authority has already issued sanctions in over 40 individual cases for violations of the GDPR), including in the context of advertising and marketing. Several enforcement actions illustrate the authority's commitment to ensuring compliance:

- (a) **IA BILET SRL:** An online ticketing platform was fined RON 9,951.40 (approximately €2,000) for sending unsolicited marketing messages without valid consent and for unlawfully deleting a user's account following their objection to direct marketing communications.
- (b) **SC Interactions Marketing SRL:** This marketing company received a fine of €1,000 for failing to implement appropriate technical and organizational measures, resulting in the disclosure of email addresses to unauthorized recipients during a marketing campaign.
- (c) **Inteligo Media:** The operator of avocatnet.ro was fined RON 42,714 (approx €9,000) for sending daily newsletters without obtaining explicit consent from users, violating GDPR provisions on lawful processing.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Romania?

N/A

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

A key topic to monitor in Romania is the draft national legislation on artificial intelligence currently under review by the Romanian Senate. This legislation seeks to ensure transparency, protect fundamental rights, and prevent misuse of AI in critical sectors such as public administration and law enforcement. Notably, it proposes prohibitions on decisions made solely by AI without human involvement in these sectors.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Companies should be aware that Romania's data protection authority, the ANSPDCP, continues to focus enforcement efforts on common areas of non-compliance, particularly in relation to unsolicited marketing, lack of proper consent, unauthorized disclosure of personal data, and failure to implement adequate security measures.

While the ANSPDCP still emphasizes corrective actions, such as warnings and remediation plans (especially for public authorities), its approach toward private entities is increasingly proactive, including through financial sanctions. Most enforcement actions arise from complaints submitted by individuals, with investigations often targeting poor documentation, misuse of legitimate interest, or unlawful profiling in marketing activities.

In practice, demonstrating compliance is just as important as achieving it. Companies should maintain up-to-date records of processing, ensure transparency in privacy notices, and audit consent mechanisms, particularly when relying on third parties or engaging in online advertising.

Although the ANSPDCP has not issued formal guidance on fine calculation thresholds, sanctions generally remain modest in amount compared to the maximum levels under the GDPR, but are increasing in frequency and are publicly reported.

In short, the trend in Romania is toward stricter scrutiny of actual practices, and organizations that handle consumer data (especially in advertising, e-commerce, or digital services) should ensure not only legal compliance but be fully prepared to face regulatory consequences in case of any breach.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

In Romania, companies face increasing pressure to keep up with evolving privacy expectations, tighter enforcement practices, and emerging regulatory developments at both EU and national levels. One of the biggest challenges is navigating complex consent requirements in digital marketing, especially in light of heightened scrutiny by the ANSPDCP over unsolicited communications and tracking technologies.

Another significant challenge is maintaining demonstrable compliance. Romanian enforcement practice places high value on documentation and accountability, which requires companies not only to comply, but to prove they comply through records, policies, and contracts.

Additionally, with the anticipated national AI legislation and increased attention to profiling, companies using automated decision-making or AI-powered marketing tools must prepare for new transparency and human oversight obligations.

Lastly, legal uncertainty and the absence of detailed local guidance in certain areas (such as legitimate interest or online behavioral advertising) create operational difficulty, forcing companies to act conservatively or seek external legal support.

12.3 What do you envision the privacy landscape will look like in five years?

Over the next five years, Romania's privacy landscape will likely become more enforcement-heavy and litigation-prone. The ANSPDCP is expected to increase the number and value of fines, and we anticipate a notable rise in lawsuits concerning unauthorized consumer data sharing, particularly in advertising and digital commerce. As privacy awareness grows, consumers will demand greater transparency and control over how their data is used, pressuring companies to adopt more user-centric consent and data management tools.

At the same time, technological shifts such as the wider adoption of biometric authentication will likely make biometric data processing more common, raising operational and compliance demands. Although already regulated as a special category of personal data under the GDPR, the increased use of biometrics will require companies to adopt stricter safeguards, conduct more frequent DPIAs, and justify necessity and proportionality more clearly.

 SLOVAKIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Slovakia.

Privacy is primarily regulated by European law, namely the EU General Data Protection Regulation ('GDPR'). For more information on the GDPR, please see the European Union chapter.

However, certain aspects of privacy are regulated by state law, in particular, Slovak Act No 18/2018 Coll on Personal Data Protection ('PDPA').

1.2 What are the primary laws regulating privacy in Slovakia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Key laws regulating privacy in Slovakia are the GDPR and the PDPA.

The GDPR is directly applicable in Slovakia and therefore most processing activities are governed by the rules and principles contained in the GDPR.

The PDPA basically complements the GDPR in cases where the GDPR does not apply to data processing, or where the GDPR leaves space for EU Member States to define categories of exceptions and derogations from the GDPR in their legal systems. The scope of the PDPA is therefore the alignment of the Slovak national legislation on data protection with the GDPR. At the same time, the PDPA reacts to several opening clauses of the GDPR and uses the option contained in the GDPR to define certain exceptions and derogations from provisions of the GDPR. The PDPA also represents a transposition into Slovak law of the EU Law Enforcement Directive (2016/680/EU). Lastly, the PDPA regulates the status, scope, and organizational structure of the Slovak data protection office ('DPA').

While the processing of personal data is governed by the GDPR and the PDPA, certain privacy aspects of online marketing activities, such as direct marketing by email or telephone, are also regulated by other laws, including in particular:

- (a) Act No 452/2011 Coll on Electronic Communications, which implements various EU law, including the ePrivacy Directive; as well as
- (b) Act No 147/2001 Coll regulating general principles of advertising, including use of personal data.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self regulation is undoubtedly an important component of the control of compliance with personal data in advertising. Slovakia is the seat of the Interactive Advertising Bureau Slovakia, the local branch of IAB Europe, which has adopted the Transparency & Consent Framework at the European level to facilitate compliance with certain provisions of the ePrivacy Directive and the GDPR.

Advertising is also self-regulated via the self-regulatory organization RPR (Rada pre Reklamu), which focuses on supervising advertising standards in Slovakia. Although bank of decisions on privacy issues of the RPR has not yet been built up, in cases of breach of general privacy rules in advertising, the RPR would be a key player to assess such conduct from a advertising perspective.

1.4 How is privacy law enforced in Slovakia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy law is enforced by the Slovak DPA, which is entitled to inspect and assess the compliance of data processing operations with the GDPR and the PDPA, and to issue orders and fines in cases where data protection laws have been violated. The Slovak DPA also publishes specific guidelines interpreting the GDPR and the PDPA. The guidelines are not binding but represent a useful source of information for entities processing personal data as well as for data subjects.

Beyond regulatory enforcement, privacy law is also enforced through judicial mechanisms. Courts in Slovakia are competent to adjudicate GDPR-related disputes, including actions initiated by data subjects, consumer protection associations, or competitors. Individuals whose rights have been infringed may seek compensation for material and non-material damages resulting from a GDPR violation. This judicial avenue serves as an essential complement to administrative enforcement by allowing affected parties to directly assert their rights. On the other hand, advertisers are also entitled to defend their rights using the administrative court system and to request judicial review of DPA decisions.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Slovakia?

See the European Union chapter.

2.2 Does privacy law in Slovakia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law also applies to foreign companies. For more information, please see the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Slovakia?

Personal data is legally defined in the GDPR which applies directly in Slovakia.

For more information please see the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

Based on one of the GDPR opening clauses, the PDPA allows the processing of genetic data, biometric data or data concerning health, and also in cases set forth in special regulations or international treaties binding upon the Slovak Republic. For example, health and genetic data may be processed within the provision of health care; biometric data can be processed for identification inside nuclear sites; and voice biometrics can be processed in the provision of banking services.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

In accordance with the GDPR, the Slovak DPA has issued a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment ('DPIA'). Among other matters, a DPIA is necessary for profiling, an assessment of credibility, or a solvency assessment. In addition to this, a DPIA is also necessary for processing biometric data for the purpose of uniquely identifying a natural person, location data, and processing using new or innovative technologies, provided that those types of processing are in conjunction with at least one other criterion (eg, scoring, or systematic monitoring) mentioned in Guidelines on DPIA (WP 248, 2017) and determining whether processing is 'likely to result in a high risk' for the purposes of the GDPR.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for the general rules.

Slovakia has adopted its own rules for telemarketing, under which marketers who conduct direct marketing by means of calls, automated dialing and communication systems without human intervention, telefax, SMS or MMS services, or persons who obtain prior consent to make calls for direct marketing purposes are obliged to use only the numbers identified by a national target code for marketing, which starts with 888. These restrictions do not apply if such marketing is conducted on publicly available numbers of entrepreneurs or legal entities, as well as if conducted on the basis of the soft opt-in exception.

Anybody in Slovakia is allowed to register their phone number in the Robinson list held by the Regulatory Authority for Electronic Communications and Postal Services to generally opt-out from marketing calls. Unless the soft opt-in exception applies, marketers cannot use a number registered in the Robinson list for marketing purposes. The sanction for such a use may be a fine ranging from €200 up to 5% of the marketer's turnover from the previous accounting period, depending on the severity of the breach.

In addition, we do have a public debate in Slovakia, as to whether so-called 'cold calling' (ie, calling to obtain consent, if the marketer had none) is possible without obtaining the prior consent of the consumer, if the cold calls are made with human intervention. Although there are voices in favor of this interpretation, we recommend careful consideration, taking into account the consent-related limitations set out in the GDPR and using a risk analysis approach.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

The Slovak DPA has stated, in its Guidance No 3/2018 on the obligations of operators of e-shops from the perspective of data privacy, that a suitable legal basis for promotions is the consent of data subject. Whilst this does not preclude the applicability of the legitimate interest of the controller or the other legal bases, it reflects the DPA's historical (yet not exhaustive and detailed) position on this issue.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

Content marketing and influencer marketing are relevant types of marketing when marketers decide to rely on different legal bases to consent for direct marketing of the data subjects when using marketing communications.

In influencer marketing, the user primarily follows the influencer and consumes their content. The social media platform mainly provides the user with the influencer's regular posts, not just sponsored content. Therefore, when the influencer shares a paid promotion, it naturally reaches their followers, who have chosen to follow that specific individual.

In contrast, in content marketing, the user primarily follows the content of a specific page or group. This could be, for instance, a Facebook page of Company A promoting its new product, or a gardening Facebook group where Company B pays to advertise a robotic lawnmower. In this case, the user is interested in the broader topic or theme, and the advertising is embedded within that content ecosystem.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

See the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

See the European Union chapter.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Slovakia? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

Although it is certainly the case that different measures need to be taken from sector to sector, the DPA has issued Decree No 158/2018 Coll on DPIA Procedure. Annex 1 to this Decree regulates the specification of security standards that companies should follow. Even though the Decree applies mainly to DPIA procedure, its annex can be used as a useful (though non-binding) tool for setting the minimum security standards of any company that starts data processing in Slovakia.

9.2 How are personal data breaches regulated in Slovakia? What are the requirements for notification and response?

See the European Union chapter.

From a practical point of view, controllers in Slovakia require processors to notify them of a data breach within 24 hours, which enables the controllers to fulfill their obligation to notify the DPA about the breach within the statutory 72 hours.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

In addition to sanctions for breach of the GDPR, the PDPA specifies sanctions for breach of those provisions of the PDPA which are based on the opening clauses of the GDPR.

Finally, according to the PDPA, the Slovak DPA may impose a procedural fine on anyone who does not cooperate during a data protection inspection.

From a practical point of view, the Slovak DPA imposed 45 fines in 2023. The total amount of imposed fines was €122,665.66, with the average fine being €2,048. The number of fines, as well as the amount of the fines, were similar to the figures from 2020–2022.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The enforcers are not very active, mainly due to a lack of personnel and resources to carry out control activities.

The Slovak DPA issues around 40–50 fines per year in total, with an average fine of €1,500–2,000. The Regulatory Authority for Electronic Communications and Postal Services handles approximately 700–800 complaints regarding unsolicited marketing calls, with the average fine for an unsolicited marketing call being around €500. The situation has not changed significantly in recent years.

The decisions related to advertising identified mostly the following breaches:

- (a) unsolicited calls;
- (b) email marketing without consent;
- (c) email marketing despite revoked consent;
- (d) unlawful data brokerage; and
- (e) storage of email addresses for marketing purposes without a legal basis.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Slovakia?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) Slovakia has currently opened discussions regarding the need to amend the PDPA with the aim of using the opening clauses of GDPR to make Slovakia’s legal environment more user-friendly for entrepreneurs.
- (b) Companies that are using cold calls with human intervention to collect data subjects’ consent for direct marketing should monitor the development of a legislative initiative to prohibit such cold calls. The draft of the bill was already open for public consultations.
- (c) Companies relying on the so-called soft opt-in exception in their direct marketing should monitor legal developments regarding the time limitation of the exception. In Slovakia, there are ongoing discussions about limiting the exception to a period of two years following the end of a commercial relationship with an existing customer who has previously been provided with similar goods or services.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Slovak DPA annually publishes its inspection plan on its official website. The plan always includes the sectors on which the Slovak DPA will focus. In 2025, it will mainly be processing activities of pharmacies, driving schools, and CCTV in restaurants. During inspections in the private sector, the DPA will focus mainly on:

- (a) principles of processing;
- (b) the legality of processing;

- (c) conditions for expressing consent;
- (d) processing of special categories of personal data;
- (e) rights of the data subjects;
- (f) joint controllers;
- (g) processors;
- (h) processing based on the authorization of the controller or processor;
- (i) personal data security;
- (j) DPIA; and
- (k) data protection officers.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Regulation of privacy continues to boom due to new technologies, in particular as a consequence of the development of AI tools and the AI market. New technologies also trigger greater interest in data subjects about their rights. This has resulted in the multiplication of data access requests and requests for the exercise of other rights. Combined, privacy is increasingly becoming a part of everyday life in every business.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Keeping track of new EU regulations (ie, the AI Act, Data Act, and other relevant regulations) and associated investments, in particular when there is a small or no budget for privacy compliance.

12.3 What do you envision the privacy landscape will look like in five years?

We expect more adequacy decisions to be adopted, since other countries outside the EEA are emerging with their own 'GDPR-like' regulations.

From the perspective of the Slovak Republic, we anticipate a continued development of case law and the imposition of higher sanctions, as data breaches in Slovakia are comparable to those in other jurisdictions, yet are sanctioned far less severely.

SPAIN

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Spain.

Privacy is a constitutional right in Spain. It is considered to be an essential and fundamental right of every Spanish citizen, and can be regulated only by organic laws, which require a special approval proceeding in the Parliament.

The Spanish Constitution provides that privacy, along with personal honor and personal image, is a fundamental right. This provision declares all personal communications to be confidential, including telephone, postal and digital communications, and restricts the use of informatics in order to protect the honor and the personal and family privacy of Spanish citizens, as well as the full exercise of their rights.

The first specific regulation about data protection was the Spanish Organic Law 15/1999, which transposed the EC Data Protection Directive into Spanish Law and established the first national governmental body with competences in this area: the Spanish Data Protection Agency ('AEPD').

In addition to the AEPD, there are other three administrations with competences on privacy law, but mainly limited to supervise regional public authorities: the Basque Data Protection Agency; the Catalanian Authority on Data Protection; and the Council of Transparency and Data Protection of Andalusia. The region of Madrid also established its own regional agency for data protection in 2005 but it was closed in 2013.

1.2 What are the primary laws regulating privacy in Spain? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The GDPR is the main source for privacy regulation in Spain, as in the rest of EU Member States.
- (b) As a consequence of the GDPR, Organic Law 15/1999 was derogated and replaced, from December 7, 2018, by the current regulation, the Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights ('LOPD'). Due to the margin of adaptation left by the European legislator to the national authorities, the Spanish LOPD has developed some particularities, including:
 - (i) a new catalogue of unfair competition practices relating the use of personal data, and a specific chapter about digital rights, regulating, eg, employees' rights to digital disconnection when they are not in working time, the right of access to the internet, the right to digital education, the principle of network neutrality, as well as the right to be forgotten, portability and rules governing the right to access a deceased person's digital content,
 - (ii) the inclusion of a person on a 'credit blacklist' is subject to specific and very strict conditions;
 - (iii) data processing agreements dated before May 25, 2018 remained valid until their expiration. If the agreement had no expiration date, it was in force until May 25, 2022.

See also discussion of the Act in later questions.
- (c) Organic Law 1/82 regulates the civil protection of honor, personal and family privacy and personal image (personality rights). In some cases, the violation of these rights might have also criminal consequences (see the Spanish Criminal Code).

- (d) The e-Commerce Law (Ley 34/2002) implemented the EC Electronic Commerce Directive and some of the provisions of EC ePrivacy Directive.
- (e) The new Audiovisual Communication Act of 2022.
- (f) the Law on General Telecommunications (Ley 9/2014).
- (g) Finally, there are a number of sectorial regulations including specific provisions about privacy, including regulations concerning consumers, unfair competition, health, insurance, employment, etc.

The Spanish data protection agency, the AEPD, is the competent authority not only to enforce legal protection against some restricted practices affecting privacy, but also regulates on, among others, anti-spam activities and e-commerce regulations.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There is no self-regulatory system relating to disputes about privacy; however, Autocontrol, the self-regulatory organization for the advertising industry, offers a pre-clearance service to comply with data protection regulations ('Data Advice'). Autocontrol also provides mediation services relating to claims about privacy.

1.4 How is privacy law enforced in Spain? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The enforcement of both the GDPR and the LOPD on a national level belongs exclusively to the AEPD, the Spanish supervisory authority. The AEPD's decisions can be appealed to the Contentious Administrative Court, and, on cassation level, to the Supreme Court. Due to the constitutional nature of privacy rights, the Constitutional Court is also entitled to review lower courts' decisions.

The role of the AEPD is not only to inspect and sanction, but also to help and guide citizens and corporations in the permanent compliance of personal data regulations, therefore, it publishes on a regular basis, guides and documents offering orientation and interpretation of the current rules. Since 2018, the Agency has published guides on, inter alia:

- (a) the use of cookies (updated in 2024);
- (b) privacy by design;
- (c) performance of risk analysis and data protection impact assessments ('DPIA's);
- (d) the use of video surveillance and biometric systems;
- (e) notification of security breaches;
- (f) the right of information;
- (g) proof of concept Blockchain and the right to erasure;
- (h) clocking and attendance control processing using biometric systems;
- (i) validation of cryptographic systems in data protection processing;
- (j) conducting a DPIA in regulatory development; and
- (k) addictive patterns and the right to the integrity of the person.

In addition, the AEPD provides a help tool, called Facilita, which helps those who process low-risk personal data to comply with the GDPR. It takes the form of an online questionnaire, taking a maximum of 20 minutes to complete, which companies and professionals can use to check that the data they process can be considered low risk and then enables them to obtain the essential documents required

to help them to comply with the GDPR. Facilita adds to other initiatives that the AEPD has launched to promote compliance with the GDPR, including the Certification Scheme for DPOs to provide security and reliability both to professional privacy enterprises and to the entities that hire their services.

The AEPD is deeply committed to protecting privacy, addressing issues such as: the use of biometric data for purposes for which it is not necessary; the protection of minors from accessing inappropriate websites; and the ability to respond quickly to reports of sexual or discriminatory abuse on social media. One example of the AEPD bringing action is the case, in 2010, against Google, brought as a consequence of a complaint from a Spanish citizen seeking to remove their name from old news indexed by this Internet engine. The case was reviewed by the CJEU (case 131/12, *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González*), which confirmed the decision against Google, and the ‘right to be forgotten’. In June 2022, the Constitutional Court confirmed the importance of this right and its scope as fundamental right.

Proceedings for enforcement of personality rights are brought before the civil and criminal courts. In such proceedings, the participation of the public prosecutor is mandatory.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Spain?

See the European Union chapter.

In addition to the scope of the GDPR, the LOPD applies to all controllers or processors who process personal data in Spain, or outside of Spain when the data referred to persons in Spain.

2.2 Does privacy law in Spain apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. According to the LOPD, the Spanish local representative of any controller or processor established outside of Spain has joint liability with the controller/processor, and the local supervisor is entitled to apply the provisions of the GDPR and LOPD to such local representative. It is not mandatory to have a local representative. However, entities required to appoint a data protection officer (‘DPO’) must ensure that the appointment is registered in the DPO list maintained by the AEPD. The appointed DPO does not need to be a Spanish national.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Spain?

Personal data is legally defined in the GDPR (see the European Union chapter).

Regarding the personal data of deceased persons, the Spanish LOPD allows successors to make use of the deceased’s right of access, and the rights to request the erasure and restriction of personal data, unless this is expressly forbidden by law or by the will of the deceased (the data subject).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Spanish LOPD does not add new categories of sensitive data to those listed in the GDPR; however it excludes the exception granted under the GDPR whereby mere consent granted by the data subject can lift the prohibition on the processing of special categories of personal data (ideology, union membership, religion, sexual orientation, race, creed, or ethnicity), in order to avoid discriminatory situations.

Additionally, situations under which data of a criminal nature may be processed are expressly regulated.

The LOPD states that the processing of personal data for purposes of preventive or occupational medicine, or public interest in the area of public health, is allowed on the grounds of public interest, but this permission must be based on a standard with the rank of law, and this law could establish additional requirements regarding security and confidentiality.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

Moreover, Spain has particular rules concerning:

- (a) **Transparency:** The right of data subjects to be informed about any processing is implemented within a granular system, in which certain minimum information (identity of the controller and its representative, the purpose for processing, the rights of the data subjects, origin of the data if they were not collected from the data subject) must be always provided in a 'first layer', with direct and immediate access available to full information on a second layer.
- (b) **Accuracy:** The Spanish Law provides some 'safe harbor' situations for a controller, whereby it will not be responsible for inaccurate data if reasonable measures to ensure deletion or rectification were taken.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The Spanish LOPD clarifies the roles established by the GDPR. In particular, a 'controller' is the person who, in its own name and without notice of acting on behalf of another, establishes relations with the data subjects, even when there is a processor's contract. This provision does not apply to processors operating within the framework of public sector contracting legislation.

Processors using data for their own purposes will be also considered as controllers.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

- (a) There is a presumption of lawful processing, based on legitimate interest, regarding the personal contact data of a person working or rendering a service (directly as individual trader or as worker of a corporation) to the controller.
- (b) There is a presumption of lawful processing, based on public interest, regarding the video surveillance systems in working places and public areas. A visible and public notice regarding the presence of cameras is compulsory. The images recorded may be used as a form of labor control of employees if they have been informed in advance. Again, if the employees have been informed in advance, the employer is entitled to access the company's digital devices used by the employees for the purpose of controlling their compliance with the employment relationship.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The minimum information to be included in the notices must be presented through a layered (or granular) information system:

- (a) The first layer of a privacy notice must be displayed at the time personal data is collected, in a way that is clear, immediate, and visible, and must contain the following minimum information:
 - (i) identity of the controller;
 - (ii) purpose(s) of the processing;
 - (iii) legal basis for the processing;
 - (iv) recipients or categories of recipients; and
 - (v) the rights of the data subject, (eg, access, rectification, deletion, etc).
- (b) The second layer must include:
 - (i) contact details of the DPO;
 - (ii) explanation of the legal basis;
 - (iii) international data transfers;
 - (iv) data retention periods;
 - (v) right to withdraw consent;
 - (vi) right to lodge a complaint;
 - (vii) source of the data (if not collected directly); and
 - (viii) automated decision-making and profiling (if applicable).

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

In addition to the individual rights granted by the GDPR, the Spanish LOPD additionally provides some minor clarifications:

- (a) The exercise of the right of access may be considered repetitive if exercised on more than one occasion during a period of six months, unless there is legitimate cause for it; and

- (b) The right of access is considered fulfilled if the controller offers data subjects means that permanently guarantees remote, direct and secure access to their personal data.

See also question 4.3 as to the presumption of lawful processing.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the Spanish E-Commerce Act, providing opt-out options is mandatory and must be available at all times to recipients. This means that every communication (eg, newsletters) must include an unsubscribe option that allows recipients to easily opt out.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

If the data shared are subject to GDPR regulation, and the assignee (third party) is not a processor working for the controller, all provisions of the GDPR relating to data transfers must be complied with.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union Chapter.

In addition:

- (a) The GDPR establishes that, where it is probable that processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller must carry out a DPIA, taking into account the origin, nature, particularity and severity of the risk. Each supervisory authority must establish the types of processing operations that require an impact assessment. Based on this, the AEPD has published a list of processing operations in which an impact assessment is mandatory. It is thus necessary to carry out an impact assessment in cases where the processing meets at least two criteria on the list, which include:
 - (i) the profiling or assessment of subjects;
 - (ii) the observation, monitoring, geolocation or control of the data subject in a systematic and exhaustive manner;
 - (iii) the use of special categories of personal data, data related to criminal convictions or data that allow to determine the economic solvency;
 - (iv) the use of biometric data to uniquely identify a person;
 - (v) the use of genetic data; and
 - (vi) the use of large-scale data.

In this way, controllers have more security when determining which processing operations are likely to result in a high risk and therefore require an impact assessment.

The list has been communicated to the European Data Protection Board, which has issued a favorable opinion on it, following the criteria established in the assessment of all the lists sent by the national authorities.

The AEPD has published another list containing those processing activities for which it is not mandatory to carry out an impact assessment.

- (b) The LOPD specifies some additional entities and bodies which have an obligation to appoint a DPO and communicate this to the AEPD. Such entities and bodies include those carrying out advertising and commercial research activities based on the data subjects' preferences or carrying out data subjects' profiling actions.
- (c) 'Data blocking', is one of legal innovations of the Spanish LOPD. Controllers are obliged to block personal data at the end of processing. This means that the data are under technical and organizational measures which avoid future processing actions but allow data disclosure if required by the competent authorities.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

In addition to regulation under the GDPR, the Spanish legal framework has some particularities arising not only from the LOPD but also from other regulations (see question 1.2). The following are the most relevant:

- (a) When consent is sought for the processing of the data for several purposes, it is necessary to state specifically and unequivocally that such consent is granted for all of these purposes.
- (b) A contract may not be made subject to the data subject consenting to the processing of their personal data for purposes that are not related to the maintenance, development or control of the contractual relationship.
- (c) From the point of view of electronic commercial communications, under the e-Commerce Law, unsolicited communications are only permitted if there is a commercial/contractual relationship with the data subject, or if express consent has been granted. An opt-out possibility must be offered in every communication. Telephone offers must be made from a telephone number duly identified; hidden numbers are prohibited.
- (d) When entities developing advertising activities and commercial inspection, including commercial research and marketing, process data based on users' preferences or elaborate users' profiles of the same, they must appoint a DPO and inform the AEPD of such appointment.
- (e) Another difference in the Spanish privacy legal framework relates to advertising exclusion systems (eg, 'Listas Robinson'), regulated specifically in the LOPD. All advertisers carrying out commercial communications must check these lists and exclude from their campaigns those data subjects who do not wish to receive commercial communications. An exception to this rule is where the affected person has previously granted consent to that particular commercial communication.
- (f) No pre-checked boxes are allowed. Consent must be positive and the consent form must always include the first layer of minimum compulsory information.
- (g) The Unfair Competition Act prohibits unsolicited and repeated offers to consumers by telephone, fax, email or other means of remote communication, except in the circumstances and to the extent that it is legally justified to enforce a contractual obligation.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There is specific guidance about cookies issued by the AEPD in November 2019 and updated in 2024. Express and positive consent is required in application of GDPR rules; It is mandatory to provide clear and complete information about the use of cookies (eg, in a banner or popup) and to allow users to accept, reject, or configure cookies easily, with equal options (no nudging).

The guidelines also recommend that ambiguous sentences or difficult legal language should be avoided, so all information provided to the user must be direct, simple, complete and transparent. The consent of minors (below 14 years old) is also covered.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs have no specific legal regulation but may be considered to be commercial relationships, which entitle the controller to process data on the basis of this consent (agreement) and allows them to send commercial communications to the client.

Sending promotions without previous consent, or without a previous commercial relationship would be a violation of both privacy and e-commerce regulations.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

This kind of advertising usually involves data processing based on users' preferences and/or elaboration of users' profiles. Any entity performing these actions must appoint a DPO who must be recorded on the AEPD's list.

On top of this, the AEPD has included this kind of data processing among those on its 'Blacklist' (based on the WP29 Guidelines) requiring a risk impact assessment and a DPIA, if the data processing allows the identification of users.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not explicitly regulated as such under Spanish privacy law, although some legislative initiatives have been discussed. AEPD is increasing the control of these practices and recommends using a granular consent model, especially in cross-device or cross-platform tracking.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

Under the LOPD, the minimum age at which any individual has capacity to give consent is fixed at 14 years.

See question 7.2 (as to use of cookies) and question 7.10 (as to profiling).

One of the latest guides published by the AEPD on ‘Design patterns used in the personal data processing of some digital products and services’ includes a special reference for minors.

The Audiovisual Communication Act restricts the use of personal data from minors when such data have been collected or otherwise generated by providers of the video sharing service through a digital platform. Those data may not be treated for commercial purposes, such as direct marketing, profiling, or personalized behavior-based advertising.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The Spanish LOPD prohibits the use of profiles for advertising purposes if they are directed to minors, and reiterates that data subjects have the right not to be subjected to decisions based solely on automated processing, including profiling, unless there are adequate additional safeguards. Therefore, all privacy notices must inform about the existence of automated decisions and profiling activities. Additionally, if the profiling is massive, a prior DPIA must be carried out.

It is worth referring to the *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* prepared by the Article 29 Data Protection Working Party and applied by the Spanish AEPD since 2018.

AEPD recommends assessing a person's participation in the decision-making process by examining different aspects, such as their authority, competence, capacity, diligence or independence. This recommendation is made taking into account the CJEU decision of 7 December 2023, ‘SCHUFA’, which established that it is also an automated decision for the purposes of the GDPR, when the automatic generation of a value from personal data is transmitted by the data controller to a third party, also a data controller, and this third party, in a decisive way, bases a decision about the person on that value.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Spain? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

In addition:

- (a) providers of telecommunication services have special duties which are regulated by the General Telecommunication Act;
- (b) the AEPD has published a guide and a software tool ('Asesora Brecha') about data security and breach which are available on its website. This guide establishes the minimum standards which do not differ by sector or size of entity; and
- (c) the LOPD provides a list of scenarios under which the adoption and implementation of technical and organizational measures is necessary, in view of the potential risks.

9.2 How are personal data breaches regulated in Spain? What are the requirements for notification and response?

In some cases, data breaches must be reported to the AEPD within 72 hours unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification can be made by the controller using standardized forms through an online system created by the Agency for this purpose (certified electronic signature is required).

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Although the GDPR does not authorize the creation of catalogues of offenses, the Spanish law provides a classification of violations and the term of statute of limitations is as follows:

- (a) **Very severe:** eg, processing without any conditions of lawfulness, failure to comply with the duty of information, international transfers without safeguards, etc. There is a 3-year limitation period for such offenses.
- (b) **Severe:** eg, processing of personal data of a minor without consent, obstruction or repeated violation of the rights of access, rectification etc). There is a 2-year limitation period for these offenses.
- (c) **Minor:** eg, failure to comply with principle of transparency of information or right of information. There is a 1-year limitation period for these offenses.

Additionally, the LOPD provides a second classification of limitation periods, according to the possible economic sanctions, whereby sanctions of €40,000 or less have a limitation period of 1 year; sanctions of €40,001–300,000 have a limitation of 2 years; and sanctions over €300,001 have a limitation period of 3 years.

All decisions and fines ruled by the AEPD are subject to a possible appeal before the Contentious Administrative jurisdiction; however, according to 2021 statistics, courts confirm the decisions of AEPD in 85% of cases.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, individuals are entitled to file claims before the AEPD both by name or anonymously, reporting violations of their own or third parties' privacy rights. Employees may also use whistleblowing reporting systems.

There several provisions regulating the whistleblowing system and setting out, eg, the controller's obligation to inform all employees about the system.

In 2023, the AEPD received 21,590 complaints, representing a 43% increase compared to 2022 and 55% more than in 2021. The complaints most frequently filed by citizens related to unsolicited advertising, internet services, video surveillance, commerce, transportation and hospitality, and financial institutions. The areas of activity with the highest fines were related to personal data breaches, financial institutions, data protection rights, fraudulent contracting, telecommunications, and internet services.

AEPD's 2024 Report indicates that 19,000 complaints were received in 2024, with AI, data spaces and neurodata among its priority challenges.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In 2023, the AEPD received 21,590 complaints, representing a 43% increase compared to 2022 and 55% more than in 2021. The complaints most frequently filed by citizens related to unsolicited advertising, internet services, video surveillance, commerce, transportation and hospitality, and financial institutions. The areas of activity with the highest fines were related to personal data breaches, financial institutions, data protection rights, fraudulent contracting, telecommunications, and internet services.

In 2024, the AEPD imposed a €10,000 fine on a digital marketing company for violating the GDPR. The company's website allowed users to submit personal data through various online forms. However, the 'Privacy and Participation Policy' that users were required to read before submitting any form provided misleading information. The link redirected users to the privacy policy of an entirely different website, unrelated to the actual owner of the site collecting the data. The AEPD confirmed that the digital marketing company's website failed to provide clear information about the actual entity responsible for handling users' personal data. Specifically, there was neither: (i) a direct link to a valid privacy policy, nor (ii) a legal notice (Aviso Legal) where such information could be found.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Spain?

The LOPD modified the Law of the General Electoral System introducing an exception for political parties, which were allowed to collect data on citizens' political opinions 'obtained in web pages and other public sources for the realization of political activities during the electoral period'. Political parties were also entitled to send electoral propaganda 'by electronic means or messaging systems', as well as through 'social networks or equivalent media', without these communications being considered commercial (ie, the e-Commerce Law did not apply).

This provision caused huge public concern and was challenged before the Constitutional Court, which declared in May 2019 that this modification of the Law of the General Electoral System was contrary to the Constitution and void.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) The protection of minors is, among others, a very relevant issue for the AEPD at this moment. A specific digital tool has been implemented for this purpose (AseguraTIC). At this moment, there are some projects ongoing for minors’ protection, such as an age verification system, which will be implemented soon and be mandatory in some areas and for some services.
- (b) The use of encryption systems can be validated using a specific tool launched in 2023 by the AEPD (‘ValidaCripto’).
- (c) It is also relevant to mention the strict interpretation by the AEPD about the use of biometric data for access control in the workplace. Such use is prohibited unless it meets the specific exceptions under the GDPR, such as legal obligations.
- (d) The implementation of European AI Act is also a hot topic. A new supervisory body, AESIA, has been created, although the AEPD will also perform some controlling and supervision competences.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

Consumers and citizens are more familiar with privacy regulations and more conscious about their rights. The number of complaints filed before the AEPD is constantly increasing and companies are investing more resources and time in privacy compliance.

On the other hand, we have also noticed a stricter approach from the controlling authorities. It’s now more usual to receive a fine of €3,000 for minor breaches (eg, incorrect or incomplete information, cookies policies, etc) and to face a fine of over €1M for, eg, using biometric systems without a proper prior DPIA.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Privacy law has become a very sensitive issue amongst consumers, employees, and citizens of all ages and walks of life. As a consequence, the number of complaints for offenses relating to privacy has increased notably. Companies must be very careful regarding marketing activities and on the alert when receiving any question or claim relating to personal data.

12.3 What do you envision the privacy landscape will look like in five years?

See the European Union chapter.

SWEDEN

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Sweden.

In Sweden, privacy is regulated by various statutory laws and regulations. For instance, the Instrument of Government, Sweden's primary constitutional law, provides provisions on the protection of individuals' privacy. In addition, other Swedish legislation, as well as EU law, also govern privacy. Furthermore, the Swedish Authority for Privacy Protection ('IMY') has issued guidelines which, although non-binding, assist practitioners in complying with privacy regulations.

Privacy has been a hot topic for a relatively long time in Sweden. Population and housing censuses carried out by public authorities in the 1970s caused debate on personal integrity, since the censuses were conducted by linking different registers kept by public authorities. Eventually, this debate led to the Swedish Government Official Report (SOU 1972:44) 'Data and Integrity'. The report proposed changes to the Swedish Freedom of the Press Act and the predecessor to the current Swedish Public Access to Information and Secrecy Act, both being statutes of importance in the field of privacy. However, and perhaps most relevant regarding the processing of personal data, the report included a proposition for a new data law, as well as introducing a new criminal offence of hacking into the Swedish Penal Code. Eventually, and prompted by the report, Sweden became the first European state to enact a law on the processing of personal data—the 1973 Swedish Data Act.

The Data Act was in force until 1998, when the Swedish Personal Data Act, based on the Data Protection Directive 95/46/EC, was enacted. The Personal Data Act was in turn repealed on May 25, 2018, when the European General Data Protection Regulation ('GDPR') entered into force. In Sweden, general supplementary provisions have been compiled in the Data Protection Act (2018:218) containing supplementary provisions to the EU Data Protection Regulation, which entered into force at the same time as the GDPR became applicable.

1.2 What are the primary laws regulating privacy in Sweden? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The GDPR is the primary legal framework governing privacy in Sweden.

In addition to the GDPR, Sweden has enacted the Data Protection Act, which is further supplemented by the Data Protection Ordinance (2018:219). The Data Protection Act serves as complementary national legislation, meaning its provisions apply where the GDPR allows or requires member states to introduce specific national rules.

Sweden has also adopted several sector-specific laws, often referred to as 'Registry Acts', which regulate personal data processing in specific areas such as law enforcement, intelligence services, finance, and healthcare. These laws primarily apply to public authorities, but certain provisions may extend to private entities depending on the nature of the processing activities and the controller involved.

Finally, the Swedish Electronic Communications Act (SFS 2022:482) ('LEK'), sometimes referred to as the 'Cookie Law,' is also relevant in the context of privacy. The LEK implements the ePrivacy Directive (2002/58/EC) and governs confidentiality, traffic and location data, and the use of cookies and similar technologies in electronic communications.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Privacy regulation is primarily governed by hard law, notably the GDPR, which sets out binding rules on how companies must process personal data—including in contexts like targeted advertising and profiling.

However, self-regulation plays a significant complementary role in promoting ethical standards, maintaining public trust, and guiding day-to-day business practices. Industry organizations such as the Swedish Advertising Ombudsman, the European Interactive Digital Advertising Alliance, and the European Advertising Standards Alliance have developed codes of conduct and best practice guidelines that advertisers are encouraged to follow. Initiatives like ‘Your Online Choices’ and the AdChoices program provide mechanisms for users to opt out of interest-based advertising, enhancing transparency and consumer control.

Additionally, IAB Europe’s Transparency & Consent Framework supports compliance with the GDPR by standardizing how advertisers and publishers obtain and manage user consent for data processing.

In Sweden, many advertisers also follow the International Chamber of Commerce Marketing Codes, adapted to the Swedish market. Self-regulation commonly addresses areas such as consent collection (especially for cookies and tracking technologies), transparency in data usage, advertising to vulnerable groups (such as children), and maintaining ethical standards beyond legal minimums.

Although self-regulatory rules are not legally binding, they serve as an important safeguard against unethical behavior. Companies breaching these standards may face public complaints, reputational harm, or negative media coverage—even if no legal violation has occurred. Repeated or serious breaches can also draw the attention of regulatory bodies like the IMY or lead to formal investigations under EU law.

1.4 How is privacy law enforced in Sweden? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Sweden has appointed the IMY as its supervisory authority for data protection. The IMY is responsible for supervising compliance with the GDPR, the Swedish Data Protection Act, the Data Protection Ordinance, and several other laws, including certain Registry Acts.

The scope of the IMY’s mandate is established by the GDPR, which requires each Member State to designate an independent public authority to monitor the application of the Regulation. In Sweden, the IMY’s responsibilities are further specified in the Regulation with Instructions for the Swedish Authority for Privacy Protection (2007:975). This Regulation outlines IMY’s mission as:

- (a) safeguarding fundamental rights and freedoms in connection with the processing of personal data;
- (b) promoting the free movement of personal data within the EU; and
- (c) supervising practices in areas such as credit reporting and debt collection.

The IMY’s powers are derived from the GDPR, which grants supervisory authorities the ability to order controllers and processors to provide information, carry out investigations including audits, and enforce compliance through warnings, reprimands, injunctions, or administrative fines.

Sweden does not have self-regulatory bodies with formal enforcement powers under privacy law. However, industry-led self-regulatory initiatives, such as those by the Swedish Advertising Ombudsman, may play a role in guiding good practices—particularly in sectors like advertising—but they do not have legal authority to enforce data protection rules.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Sweden?

See the European Union chapter regarding which companies are subject to the GDPR.

The Swedish Data Protection Act applies to:

- (a) the processing of personal data carried out by a controller or processor established in Sweden;
- (b) the processing of personal data by a controller not established in Sweden, but in a location where Swedish law applies pursuant to international law; or
- (c) the processing of personal data by a controller or processor established in a third country, if the processing concerns data subjects located in Sweden, and if the processing is related to either the offering of goods or services to such data subjects or the monitoring of their behavior within Sweden.

The territorial scope of the Data Protection Act closely mirrors that set out in the GDPR, but with Sweden as the territorial reference point rather than the European Union. Consequently, a company established outside Sweden may still be subject to the Data Protection Act if its activities fall within this scope.

In addition, the Registry Acts have varying scopes of application, each tailored to the specific sector they regulate.

2.2 Does privacy law in Sweden apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law in Sweden can apply to companies outside Sweden. See question 2.1.

Swedish law does not set out any requirement to have a company representative in Sweden.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Sweden?

The Swedish Data Protection Act and the Registry Acts adopt the definition of personal data set out in the GDPR. Accordingly, the Swedish definition of ‘personal data’ is identical to that in the GDPR. See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

In Sweden, special categories of personal data and sensitive personal data are defined as provided by the GDPR. See the European Union chapter.

The Data Protection Act sets out provisions relevant to the processing of certain categories of sensitive personal data. It provides several exceptions to the general prohibition on processing sensitive personal data set out in the GDPR. These exceptions apply to sensitive personal data processed within the fields of employment, social security and social protection law. One such exception is that an employer may process sensitive personal data about its employees for the purposes of fulfilling its obligations under labor, social security or social protection law, without the employee's consent.

In Sweden, each Swedish citizen (as well as non-citizens in some situations) has their own personal identification number used to identify the individual. While its use is widely accepted and less controversial in Sweden than in some other EU Member States, it is subject to special protection under the Data Protection Act, which states that personal identity numbers may only be processed without the data subject's consent if the processing is justified, considering:

- (a) the purpose of the processing;
- (b) the importance of a safe identification; or
- (c) any other weighty reason.

Regarding children's personal data, the Data Protection Act provides that, when offering information society services to a child domiciled in Sweden, processing is lawful based on the child's own consent only if the child is at least 13 years old. If the child is under 13, consent must be given or authorized by a holder of parental responsibility. Sweden thus applies the lowest age threshold permitted under the GDPR for children's consent in digital services. See also question 7.9.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under Swedish privacy law, aligned with the GDPR, the treatment of data depends on whether it can still be linked to an identifiable natural person.

Anonymized data refers to information that has been irreversibly stripped of all personal identifiers, such that re-identification is no longer possible, even when combined with other reasonably available data. Truly anonymized data is no longer considered personal data and thus falls outside the scope of the GDPR and Swedish privacy law. However, the IMY applies a strict standard, requiring both legal and technical safeguards that eliminate any realistic possibility of re-identification.

Pseudonymization involves replacing personal identifiers with codes or aliases while keeping the means of re-identification separately stored and protected. Because re-identification remains theoretically possible, pseudonymized data continues to qualify as personal data under both the GDPR and the Swedish Data Protection Act. As such, it remains fully subject to data protection obligations. Nonetheless, pseudonymization is recognized as a risk-reducing safeguard, particularly relevant when assessing security measures and breach notification requirements.

The broader term **de-identified data** may refer to either anonymized or pseudonymized data, depending on the method and effectiveness of the de-identification. Under Swedish privacy law, consistent with GDPR principles, the key factor is whether re-identification is realistically possible. If it is, the data is still personal data and subject to regulation. If re-identification is impossible, the data is considered anonymized and excluded from the GDPR and the Data Protection Act.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Obligations vary based on the companies' services, data type and volume, and the size of the company. There is, for example, an obligation to provide information of when and what personal data is collected, and controllers must ensure that data subjects can exercise their rights, such as the right to access and erase data processing.

For more information on the key obligations for companies under privacy law, see the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

For detailed information on the respective obligations of controllers and processors, see the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, the GDPR requires that all processing of personal data must be based on one of the six lawful bases. See the European Union chapter.

The Data Protection Act contains supplementary provisions, including rules on offering information society services directly to children residing in Sweden. According to the Act, the processing of personal data is permitted with the child's consent, provided that the child is at least 13 years old. See question 7.9.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the GDPR companies processing personal data for advertising purposes must provide clear, transparent, and accessible privacy notices. For a detailed overview of the GDPR requirements, including information to be included in privacy notices such as identity of the controller, legal basis for processing, retention periods, data subject rights, and use of profiling, see the European Union chapter.

Under Swedish law, these requirements are further supported by the Data Protection Act and enforced by the IMY. The IMY has issued guidance emphasizing the importance of clear and understandable language, especially in the context of digital marketing and when targeting children or other vulnerable groups.

Sweden has also implemented the LEK, which incorporates provisions from the ePrivacy Directive. This law applies specifically to the use of cookies and similar tracking technologies and requires informed consent prior to placing such technologies on a user's device, unless strictly necessary for the service. As such, privacy notices in Sweden should also clearly inform users about cookie usage, tracking technologies, and how consent is obtained and managed.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Under the GDPR, consumers have several important rights regarding the processing of their personal data for advertising purposes. These rights promote transparency, control, and protection against misuse of personal information. For a full list and explanation of these rights, such as the right to be informed, right of access, right to rectification and erasure, right to restrict or object to processing, data portability, and protection from automated decision-making see the European Union chapter.

In Sweden, these rights are enforced by the IMY, which provides guidance and handles complaints from individuals whose rights under the GDPR may have been infringed. Companies operating in Sweden must therefore ensure that they have practical procedures in place to respond to data subject requests in accordance with the GDPR, including timely and transparent communication.

Additionally, when personal data is processed for direct marketing purposes, Swedish practice reinforces the individual's absolute right to object, and the IMY has emphasized the importance of clearly informing individuals of this right in all marketing-related contexts.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the GDPR and the ePrivacy Directive, companies must obtain consent or provide opt-out mechanisms for advertising activities depending on the nature of the data processing involved. For more information regarding this, see the European Union chapter.

In addition to the GDPR, the Swedish Marketing Practices Act (2008:486) sets out provisions relevant for marketing via email, fax or telephone. A trader may, when performing marketing measures towards natural persons, use email, fax or automatic calling devices or any other similar automatic system for individual communication not operated by an individual, only if the natural person has given prior consent. The Act sets out exceptions to this general rule, meaning that consent is not always required. If the trader has received the natural person's electronic address for electronic mail in conjunction with the sale of the trader's products, the consent requirement does not apply if the following items are fulfilled:

- (a) the natural person has not objected to the use of the electronic address for the purpose of marketing via electronic mail;
- (b) the marketing measure relates to the trader's own similar products; and
- (c) the natural person is clearly and explicitly given the opportunity to object, simply and without cost, to the use of such electronic address for marketing purposes, when the electronic address is collected, as well as upon any subsequent marketing measure.

Regarding processing of personal data for direct marketing purposes, Swedish case law (although based on the repealed Personal Data Act) states that traders may use personal data to send marketing messages to natural persons if there is an active relationship between the organization and the natural person. Also following from case law, organizations may, at least generally, process personal data for one year from the date on which the purpose for which the personal data was collected was fulfilled. It is notable that a trader may only process the personal data for specific purposes. For instance, the IMY has stated that a retailer selling sporting gear may keep information about its customers to perform direct marketing measures aimed at the data subject regarding the retailer's similar products.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The requirements outlined in the European Union chapter apply equally in Sweden, as the GDPR is directly applicable.

In the Swedish context, one important addition is the application of the ePrivacy Directive, implemented nationally through the LEK. Vendors and third parties in advertising frequently rely on technologies such as cookies, tracking pixels, and device fingerprinting to collect data about users, and this legislation governs the use of such tracking technologies. Under Swedish law, prior informed consent is required before any non-essential cookies or similar technologies are placed or accessed on a user's device, regardless of whether the information collected is considered personal data under the GDPR.

This requirement has direct implications for how advertising-related vendors operate in Sweden. Advertisers and publishers are responsible for ensuring that valid consent is obtained, even when the tracking or data collection is performed by third parties. As such, organizations must coordinate closely with their vendors to ensure compliant consent mechanisms are implemented.

The IMY actively enforces these rules. In its decision 2023-16453 concerning ATG, IMY reprimanded the company for deploying a cookie banner that made it easier for users to accept cookies than to reject them. The design was found to mislead users and thereby violated the requirements of the GDPR, as the consent collected was neither freely given nor sufficiently informed. This case illustrates how both GDPR and Swedish ePrivacy rules are applied together in the context of advertising technologies involving third-party vendors.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

In Sweden, the contractual obligations described under the GDPR apply fully and without material deviation. See the European Union chapter.

However, companies operating in Sweden should also be aware of local supervisory expectations and guidance from the IMY. While the formal requirements stem from the GDPR, the IMY has issued guidance emphasizing the importance of clearly defining roles and responsibilities between controllers and processors. According to the IMY, controllers must ensure that processors offer sufficient guarantees regarding technical and organizational measures, and that agreements clearly document the scope of processing and the controller's instructions.

Additionally, the IMY expects that documentation be thorough and specific, especially in complex ecosystems such as advertising technologies or cloud service chains where accountability and data flows may be difficult to track. For international data transfers, companies must implement safeguards like Standard Contractual Clauses ('SCC's) and assess whether adequate protection can be ensured in the destination country. This obligation follows from the CJEU judgment in Schrems II (C-311/18), which invalidated the EU-US Privacy Shield and clarified that SCCs are only valid where they are supported by effective supplementary measures and transfer impact assessments, particularly when transferring data to countries without an EU adequacy decision.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies should, for the purpose of assessing compliance with the GDPR, consider that the engagement of processors should not lower the level of protection for the rights of data subjects compared to a situation where the processing is carried out directly by the controller. This refers to the engagement of the initial processor, but also to the engagement of additional processors along the processing chain, eg sub-processors and sub-sub-processors. Companies should therefore exercise due diligence in their selection of and oversight over their processors.

As regards the requirement to conduct impact assessments, it can be noted that the IMY has clarified nine criteria, any two of which being met entailing the need for an impact assessment. For example, impact assessments would be required for the following advertising uses:

- (a) a company uses its customers' location data, obtained, for example, via an app, for the purpose of targeting advertising to the customer or planning its advertising strategies;
- (b) a company collects data from social media to profile individuals and then target advertising to certain selected groups; or
- (c) an internet search engine collects data about individuals who use the service to create customer profiles and targeted advertising.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

In Sweden, direct marketing through emails, text messages, and push notifications is regulated under both national and EU privacy laws, primarily the GDPR, the Swedish Marketing Act, and the LEK.

As detailed in the European Union chapter, the GDPR and the ePrivacy Directive establish the overarching rules for direct marketing across the EU.

In addition to EU regulations, Sweden has specific laws that govern direct marketing. Under the Swedish Marketing Act, unsolicited electronic marketing to individuals generally requires prior consent. However, if a company has obtained an individual's contact details in the context of a sale, it may send marketing communications about similar products or services without additional consent, provided that:

- (a) the individual has not objected to such use of their contact information, and
- (b) the individual is clearly and explicitly given the opportunity to opt out, both at the time of data collection and with each subsequent marketing communication.

Furthermore, all marketing communications must include a valid address or method for the recipient to opt out of future marketing.

The LEK is directly relevant to direct marketing because it governs the use of cookies and similar technologies that are commonly employed for tracking and profiling users for marketing purposes. Storing or accessing information on a user's device, such as through cookies, is only permitted if the user has been informed about the purpose of the processing and has given their consent.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter regarding processing of personal data.

When using tracking technologies, compliance with the LEK may be required. The LEK sets out provisions relevant for the use of cookies and other technologies where information is stored in or retrieved from terminal equipment. Information may be stored in, or retrieved from, a subscriber's or a user's terminal equipment (eg, use of cookies) only if the subscriber/user is provided with access to information on the purposes for the processing and if has given consent to it. This does not apply to:

- (a) the storage or retrieval necessary for the transmission of an electronic message via an electronic communications network; or
- (b) storage or retrieval necessary to make available a service explicitly requested by the user/subscriber.

The LEK does not give detailed information regarding how to give users or subscribers access to information and how to obtain a valid consent; but, from a general point of view, a consent for cookies is subject to the same requirements that apply to a valid consent under the GDPR.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions that process personal data must comply with the GDPR and, where applicable, the ePrivacy Directive.

For further information, see the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing are subject to privacy regulation under the GDPR, the Swedish Data Protection Act, and, in relevant cases, the LEK.

When influencers or companies use personal data, such as names, contact details, location data, IP addresses, or behavioral information for marketing purposes, the GDPR applies. This includes activities like running giveaways, tracking user engagement, or targeting followers using analytics tools. Anyone who determines the purpose and means of such processing qualifies as a data controller and must ensure there is a valid legal basis for the processing, such as consent or legitimate interest. They must also provide clear privacy notices, uphold individuals' rights under the GDPR, and apply principles such as data minimization and purpose limitation. For more information, see the European Union chapter.

In cases where cookies, pixels, or similar tracking technologies are used, for example, to collect marketing data or retarget users, the rules in the LEK also apply. According to the LEK, such technologies may only be used if the individual is informed of the purpose and has given prior consent, unless the technology is strictly necessary for providing a requested service. This is particularly relevant for influencers and marketers who embed third-party tools like the Meta Pixel or TikTok Analytics into their pages or links.

Moreover, when influencers use platform tools provided by companies like Instagram, TikTok, or Facebook, they may share data protection responsibilities with the platform. In such cases, both parties can be regarded as joint controllers, as clarified in case law from the CJEU (eg, Case C-210/16, *Wirtschaftsakademie*).

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Under the GDPR and the ePrivacy Directive, any targeted or behavioral advertising that relies on tracking or profiling users triggers strict consent and transparency requirements. Companies must have a valid legal basis (usually the user's informed consent) to process personal data for personalized ads, and they must clearly inform users about the data collected and its use. The GDPR applies a more lenient approach to contextual advertising. See the European Union chapter for more context.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Swedish privacy law does not contain specific rules on digital identity resolution or clean room technologies beyond the general framework established under the GDPR and the ePrivacy Directive, as discussed in the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising falls under the scope of the GDPR and the ePrivacy Directive, as it typically involves the processing of personal data through tracking technologies. Processing location data for advertising purposes generally requires explicit consent, particularly for precise geolocation. Legitimate interest may be invoked in limited cases, but only after a balancing test and with clear opt-out options for users. For more information, see the European Union chapter.

Under the LEK, under provisions which implement the ePrivacy Directive, prior consent is also required if location data is collected using cookies, Wi-Fi, Bluetooth, or GPS through terminal equipment. Such consent must meet GDPR standards—it must be freely given, specific, informed, unambiguous, and revocable.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising directed at children and minors is strictly regulated through a combination of privacy, consumer protection, and marketing laws due to the need to protect children's personal integrity and vulnerability in commercial settings.

Under the GDPR, children are considered a particularly vulnerable group whose personal data warrants special protection, see the European Union chapter. The GDPR allows Member States to set the age at which children can lawfully consent to the processing of their personal data in relation to information society services, Sweden has set this age at 13 years. This is regulated in the Swedish Data Protection Act, and means that verifiable parental consent is required when processing personal data for advertising purposes—especially in online environments.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

In Sweden, the use of profiling, artificial intelligence ('AI'), and automated decision-making for advertising is subject to strict regulation under the GDPR and supplemented by national laws and guidance from the IMY. Profiling—defined under the GDPR as any form of automated processing of

personal data to evaluate personal aspects such as behavior or preferences—is widely used in digital advertising. However, this type of data processing requires a valid legal basis, typically explicit consent, especially when the profiling is extensive or involves behavioral tracking. In limited cases, legitimate interest may be relied on, but only after a thorough balancing test that considers the privacy impact on individuals.

When profiling involves automated decision-making that produces legal effects or similarly significant consequences for the individual (such as excluding users from offers or manipulating pricing), the GDPR imposes additional restrictions. Individuals have the right not to be subject to such decisions unless they are necessary for a contract, authorized by law, or based on explicit consent. Even in those cases, the organization must provide meaningful information about the logic involved, ensure human oversight, and offer the right to contest the decision. For more information see the European Union chapter.

The IMY has issued guidance emphasizing the need for transparency, fairness, and accountability in profiling and AI-based advertising. In a notable case against Bonnier News AB (DI-2019-11737), the IMY found that the company had unlawfully profiled users for advertising purposes without a valid legal basis and without proper transparency. Bonnier had relied on legitimate interest, but the IMY ruled that this was insufficient due to the extent of data collected and the nature of the profiling. The IMY also concluded that the use of cookies and similar tracking technologies required prior consent, as mandated by the LEK. As a result, Bonnier News AB was fined SEK 13 million (approx €1.36 million) for breaches of the GDPR and ePrivacy rules.

In addition, the EU Artificial Intelligence Act ('AI Act'), adopted in 2024, introduces specific obligations for AI systems used in advertising. While most advertising-related AI systems will not be considered 'high-risk,' they must still comply with transparency obligations under the AI Act, such as informing individuals that they are interacting with an AI system or being subject to AI-driven content personalization. For example, when AI is used to generate or target ads based on profiling, users must be clearly informed. Furthermore, providers and deployers of AI systems must ensure the systems are safe, technically robust, and respect fundamental rights, including data protection and non-discrimination.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The requirements described above, for data transfers, apply to discovery or similar proceedings.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Sweden? Are there minimum standards? Does this differ by sector or size of the entity?

Data security in Sweden is regulated primarily through the GDPR, which requires all organizations processing personal data to implement appropriate technical and organizational measures to ensure data confidentiality, integrity, and availability. These measures must be risk-based and regularly updated. Unlike data protection, data security extends beyond personal data and applies to all types of sensitive information. Examples include encryption, pseudonymization, access controls, system resilience, secure disposal of data, and clean desk policies. Organizations must also perform ongoing risk assessments and vulnerability testing.

The IMY has stated that it will not provide detailed instructions for controllers or processors on the specific security measures needed to comply with the GDPR. Instead, it has issued non-binding guidelines, intended as recommendations rather than definitive compliance checklists. According to these guidelines, controllers and processors must be aware of the personal data they process, ensure transparency in their data handling (for example, through privacy policies), rigorously maintain required documentation, and continuously conduct impact assessments and vulnerability tests to uphold GDPR security standards.

The specific security measures required may vary depending on the sector and the size of the entity. Organizations operating in high-risk sectors, such as healthcare, finance, or telecommunications, are generally expected to implement more stringent security measures, often based on additional sector-specific regulations. Similarly, larger organizations or those processing sensitive or large volumes of personal data are held to higher security expectations, whereas smaller companies may meet requirements with more basic, risk-appropriate safeguards.

9.2 How are personal data breaches regulated in Sweden? What are the requirements for notification and response?

Under Swedish law, personal data breaches are regulated primarily through the GDPR, but for certain sectors, particularly providers of public electronic communications networks and services, the LEK imposes additional obligations.

While the GDPR governs breach notification generally, the LEK operates as *lex specialis* in the telecommunications sector, meaning it takes precedence over GDPR where the provisions overlap. According to the LEK, providers must immediately notify the Swedish Post and Telecom Authority ('PTS') if a security incident occurs. A security incident is defined as an event leading to unauthorized access to, or the loss, destruction, or alteration of, data processed in the course of offering public electronic communication services. If the incident is likely to negatively affect users or subscribers, such as through a compromise of their personal privacy or data integrity, the provider must also notify those affected without undue delay. The PTS may additionally require such notification.

In practice, challenges can arise in determining whether an incident should be reported to the PTS under the LEK or to the IMY under the GDPR. To address this, the PTS has issued non-binding guidance. The general principle is that if the breach falls within the scope of LEK, it must be reported to the PTS and not to the IMY. Only breaches outside the LEK's scope, such as those involving internal systems

not subject to public electronic communication regulation should be reported to the IMY in accordance with the GDPR. This division of responsibility ensures that security incidents in the telecom sector are subject to tailored oversight while maintaining consistency with broader European data protection principles.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Non-compliance with the GDPR can lead to serious consequences, including administrative fines, corrective orders, civil liability, and, in some Member States, criminal penalties. Fines can reach up to €20 million or 4% of global annual turnover, depending on the severity of the violation. Data protection authorities may also impose warnings, reprimands, or processing bans. Individuals have the right to claim compensation for damages resulting from violations. Regulatory enforcement has intensified, highlighting the importance of strong compliance frameworks.

For more detailed information, see the European Union chapter.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers have a private right of action and access to several remedies when their data protection rights are violated. Individuals can file a complaint with the IMY, which is responsible for supervising compliance with the GDPR and national data protection rules. The IMY may investigate the matter, issue warnings, impose administrative fines, or order the organization to take corrective measures.

In addition to regulatory remedies, individuals also have access to judicial remedies. They can appeal the IMY's decisions to the Administrative Court in Stockholm or bring claims directly before the general courts against a controller or processor that has violated their rights under the GDPR. This includes the right to claim compensation for both material and non-material damages caused by unlawful processing of personal data, as set out in the GDPR. Liability may apply to both the controller and the processor, depending on the circumstances.

While Sweden does not have a broad class action system for privacy-related cases, certain types of collective actions may be brought by qualified consumer or advocacy organizations under the Law on Group Actions or pursuant to EU collective redress mechanisms.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The IMY has demonstrated increasing activity in enforcing privacy regulations, particularly concerning advertising practices. While Sweden's enforcement landscape may not be as aggressive as some other EU countries, recent years have seen a notable uptick in actions targeting companies for GDPR non-compliance in the advertising sector.

Notable enforcement actions in advertising contexts are Case No IMY-2022-3270, where IMY fined Apoteket AB SEK 37 million (approx €3.4 million), and Case No IMY-2022-3271, where IMY fined Apohem AB SEK 8 million (approx €740,000), both for GDPR violations related to their use of the Meta Pixel on their websites. The pharmacies collected more personal data than necessary and unlawfully

transferred sensitive information to Meta for marketing purposes. Further examples include Case No DI-2020-10545, where IMY fined H&M SEK 350,000 (approx €32,294) for making it unnecessarily difficult for individuals to object to direct marketing communications, and Case No DI-2019-11737, where Bonnier News AB was fined SEK 13 million (approx €1.2 million) for unlawfully profiling users and sharing personal data for behavioral advertising without a valid legal basis. Additionally, in Case No DI-2019-6696, Spotify AB was fined SEK 58 million (approx €5.35 million) for failing to provide clear and comprehensive information about its processing of personal data, particularly in the context of personalized advertising services.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Sweden?

The principle of public access to official records has been incorporated into the Freedom of the Press Act. The principle applies to public authorities. This means that any person (regardless of citizenship) has the right to study official records kept by a public authority.

The GDPR does not prevent personal data in public records from being transferred to an individual making a request to study an official record. If the public authority transfers the official record, which includes personal data, it must nevertheless comply with certain provisions of the GDPR. For instance, if the public record includes sensitive personal data, the public authority must take appropriate safeguards to compensate for the infringement the transfer means for the data subject.

In certain situations, the general marketing rules under the Marketing Practices Act could also apply to privacy-related matters. For instance, it has been argued that a breach of privacy could sometimes be considered as an unfair marketing measure, depending on the circumstances surrounding the breach.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

As is the case in many other Member States, a hot topic in Sweden is the draft ePrivacy Regulation, which would, among other things, replace the LEK. See the European Union chapter.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The privacy landscape has evolved in response to the development and widespread use of new technologies, particularly artificial intelligence. Most notably, the European Union has adopted the AI Act, which sets out comprehensive requirements for the use of AI systems.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

One of the biggest challenges companies face is determining which rules and regulations apply to their operations, especially in relation to new technologies. Another challenge is ensuring compliance with privacy regulations across multiple jurisdictions, especially for companies with operations across many regions. Such companies must adhere to various new regulations and implement practices which comply with privacy regulations across all applicable regions.

12.3 What do you envision the privacy landscape will look like in five years?

We anticipate that in the years to come there will be more guiding judgements regarding the interpretation of new regulatory frameworks, such as the EU AI Act.

GHANA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Ghana.

In Ghana, privacy is regulated by the 1992 Constitution of the Republic of Ghana ('Constitution') and Acts of Parliament, including Act 843, Data Protection Act 2012 ('Data Protection Act').

1.2 What are the primary laws regulating privacy in Ghana? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The Constitution contains principles that recognize and protect the right to privacy of its citizens. It provides for the privacy of individuals, and that this right should not be interfered with except in accordance with the law, for public safety, economic wellbeing of the country, health or moral reasons, or for the prevention of crime and/or protection of others.
- (b) The Data Protection Act is the principal Act which protects the privacy of the individual and personal data and regulates the processing of personal information.

There are also laws which are sector-specific and impact data protection/privacy in Ghana. These include:

- (c) Act 775, the Electronic Communications Act 2008 ('Electronic Communications Act') as amended; as well as
- (d) Electronic Communications Regulations 2011 (LI 1991) ('Electronic Communications Regulations').

In addition, there are laws which regulate advertising in specific sectors such as public health, food, drugs, cosmetics, gaming and electronic transactions.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays an important role in privacy regulation, especially when it comes to advertising, by encouraging companies to adopt ethical practices without solely depending on rules and regulations laid down by the government and existing regulatory authorities.

For instance, the industry self-regulator, the Advertising Association of Ghana ('AAG') regulates the activities of its members through its Code of Professional Conduct and Ethics ('Code'). It lays down principles that guide content accuracy and fairness in advertising amongst other things and takes measures to ensure members comply with the provisions of its Code in relation to privacy in advertising. Its scope is limited to its members only.

1.4 How is privacy law enforced in Ghana? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy law is enforced by the Data Protection Commission ('DPC'), which is a body set up by the Data Protection Act for this purpose.

In addition, electronic communications are regulated by the National Communications Authority ('NCA').

The DPC and NCA are government regulators through which privacy law is enforced in line with the enforcement provisions of the relevant statutes.

There is also the AAG, the industry self-regulator, which can issue warnings to concerned parties or recommend relevant steps or measures which the concerned parties may take to make them compliant. This may include effecting particular changes to advertising content to bring them in compliance with its Code or applicable advertising practices, and correct any breaches contained in such content. The AAG, as a way to keep members in check, may suspend or expel non-compliant members who persistently breach its Code.

The Constitution provides for the breach of a person's fundamental rights. Thus, a private individual whose privacy/fundamental rights have been infringed by way of advertising practices or content may approach the High Court for appropriate remedies.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Ghana?

The Data Protection Act provides that a data controller may not process personal data unless it has been registered under the Act. Such registration is renewable every 2 years.

A 'data controller' is defined as a person who either alone, or jointly with other persons, or as a statutory duty, determines the purpose for, and the manner in which, personal data is processed or is to be processed. Thus, any company that, as a statutory duty, determines the purpose for, and the manner in which, personal data is processed or is to be processed will be subject to privacy laws.

2.2 Does privacy law in Ghana apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Data Protection Act applies to persons/companies outside Ghana in the following circumstances:

- (a) the data controller is established in Ghana and the data is processed in Ghana;
- (b) the data controller is not established in Ghana, but uses equipment or a data processor carrying on business in Ghana to process the data; or
- (c) processing is in respect of information which originates partly or wholly from Ghana.

All data controllers are required to register with the DPC. Those not incorporated in Ghana must register as an external company.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Ghana?

The Data Protection Act defines 'personal data' as data about an individual where the individual can be identified either from the data, or from the data or other information in the possession of, or likely to come into the possession of, the data controller.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Data Protection Act defines ‘special personal data’ as personal data which consists of information that relates to:

- (a) the race, color, ethnic or tribal origin of the data subject;
- (b) the political opinion of the data subject;
- (c) the religious beliefs or other beliefs of a similar nature of the data subject;
- (d) the physical, medical, mental health or mental condition or DNA of the data subject;
- (e) the sexual orientation of the data subject;
- (f) the commission or alleged commission of an offence by the individual; or
- (g) proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in the proceedings.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The Data Protection Act, which outlines the principles for processing personal data, does not explicitly refer to anonymization, pseudonymized or de-identified data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The Data Protection Act requires companies to observe the following in relation to processing data to protect privacy rights of data subjects:

- (a) Personal data should be processed without infringing the privacy rights of the data subject and should be done in a lawful and reasonable manner.
- (b) Personal data may only be processed for a purpose that is necessary, relevant and not excessive.
- (c) Consent of the data subject is required to process personal data, unless it is for the purpose of a contract, required by law, for the performance of a statutory duty or to protect the legitimate interest of the data subject or data controller.

The DPC also mandates that the data controller must appoint a data protection supervisor (‘DPS’) whose responsibility is to monitor the data controller’s compliance with the provisions of the Data Protection Act. The data controller is also obligated to provide adequate training to its DPS, who must be certified by the DPC. The DPC conducts the training of the DPS upon its appointment, and evidence of the DPS training and certification by the DPC is a requirement for renewal of a company’s registration with the DPC.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. The Data Protection Act differentiates a data processor from a data controller as follows:

- (a) A **data controller** is a person who either alone, or jointly with other persons, or as a statutory duty, determines the purpose or the manner in which personal data is processed or to be processed.

The data controller bears responsibility for the data that is being processed on its behalf, as it is the entity registered with the DPC and will be held liable in the event of a breach under the Data Protection Act. The data controller is obligated to register with the DPC within 20 days of commencement of business and obligated to ensure that personal data is processed fairly, transparently and lawfully.

- (b) A **data processor** is any person other than an employee of the data controller who processes the data on behalf of the data controller.

The data processor's obligations include acting in accordance with the instructions provided by the data controller, implementing technical and organizational measures which are appropriate to ensure data security, and maintaining confidentiality of personal data which they process.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Ghana's privacy law requires a lawful basis for processing personal data. The Data Protection Act requires that all processing of personal data should be carried out in a lawful and fair manner, while ensuring that the privacy rights of data subjects are not violated.

Under the Data Protection Act, consent of data subjects must be obtained by the data controller before processing their personal data, unless the purpose for which the data is being processed falls under one of the exceptions stipulated in the Act. These include where the processing is:

- (a) authorized by law,
- (b) necessary for the purpose of a contract to which the data subject is a party,
- (c) for performance of a statutory duty, or
- (d) to protect the legitimate interests of the data controller or a third party, provided it does not override the fundamental rights and freedoms of the data subject.

The Data Protection Act also gives the data subject the right to object to the processing of personal data unless the law provides otherwise.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Companies processing personal data for advertising purposes must ensure that the notices conform with the provisions of the Data Protection Act. The privacy notices should include the following information:

- (a) the nature of the personal data being collected;
- (b) the name and address of the data controller responsible for collecting the data;
- (c) the specific purpose for collecting the data, which in this case would be advertising;
- (d) whether providing the data is optional or mandatory for the individual;
- (e) if there are any consequences for failing to provide the data;
- (f) the recipient of the data; and
- (g) the existence of the data subject's right to access or request rectification of the data collected before collection commences.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Data subjects (which term include consumers) have some rights with respect to their personal data in advertising contexts which include:

- (a) **Right to consent:** Data controllers must obtain prior written consent from consumers before using their personal data for direct marketing purposes.
- (b) **Right to object:** Consumers have the right to object at any time, without providing a reason for the objection, to the processing of their personal data for direct marketing purposes, including profiling related to such marketing. This can be done by giving written notice to the data controller.
- (c) **Right to be informed:** Consumers must be informed about the nature of their personal data being collected, the purpose of collection, and the recipients who will have access to the data.
- (d) **Right to lodge complaint:** Consumers, being data subjects, have the right to complain in writing to the DPC where their rights are being breached under the Data Protection Act.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

The Data Protection Act mandates companies to obtain the prior written consent of individuals before using their personal data for direct marketing purposes. This applies to all forms of direct marketing, including email, SMS, and other electronic communications.

Moreover, under the Electronic Transactions Act, senders/companies are obligated to provide an option to cancel or opt out from a subscription in every subsequent marketing message, allowing users to withdraw their consent at any time. Recipients of such electronic marketing communications are entitled to be notified about the source from which their personal information was obtained.

Also, a company cannot assume that an agreement has been concluded with a customer who has not responded to any unsolicited communication. Any such customer will be entitled to the recovery of costs associated with cancelling or terminating such unsolicited communication.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The Data Protection Act does not specifically address the use of vendors and other third parties in advertising. However, the general obligations on data controllers, who are primarily responsible for ensuring compliance with data protection laws, even when using third-party vendors, will apply.

Data controllers must obtain prior written consent from individuals before using their personal data for direct marketing purposes, including when making use of third parties.

Data processors and third parties acting on behalf of the data controller must process personal data only with prior knowledge or authorization of, and according to the instructions provided by, the data controller. Data processors must keep the data confidential and process it in line with the DPC's data protection principles.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The processing of personal data by a data processor for a data controller must be governed by a written contract. There must be confidentiality, and the data processor must ensure security and integrity of the personal data. The contract should include provisions to maintain the confidentiality of all personal information and prohibit disclosure to unauthorized third parties. These contractual requirements are designed to ensure that personal data is protected and processed in line with applicable data protection laws while complying with the provisions of the Data Protection Act. These requirements apply whether the data is managed by the company directly or by its vendors and third-party partners.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies are required to register with the DPC as data controllers and some key documents, information and conditions are required to be provided and met before the registration is approved by the DPC. This registration must be renewed every two years.

Where an applicant provides false information to the DPC in support of its application for registration as a data controller, that applicant commits an offence and will be liable upon conviction to a fine of not more than one hundred and fifty penalty units (GH¢1800 (approx USD 116.13)) and/or a term of imprisonment of not more than one year.

The Data Protection Act also requires companies to ensure that they have a valid legal reason (such as consent, contractual necessity, or legitimate interests) before processing personal data. Consent is required for direct marketing, unless there is legal exemption.

Note however that the Data Protection Act does not explicitly mandate the carrying out of an impact assessment for advertising uses.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Electronic communications are regulated by the Electronic Communications Act and the Electronic Communications Regulations.

The Electronic Communications Regulations provide for privacy and secrecy in electronic communications. People, other than the sender or intended recipient, who steal, intercept, alter, divert or unlawfully disclose transmitted messages or data commit an offence and are liable on summary conviction to a fine of not more than 500 penalty units (approx GH¢ 6,000 (USD 738)) and/or a term of imprisonment of not more than 5 years.

Moreover, operators must employ international best practices in the industry to promote the privacy, secrecy and security of communications transmitted by them or through their systems, as well as personal and account data related to subscribers. Anyone who breaches this is liable to a fine of not more than 500 penalty units (approx GH¢ 6,000 (USD 738)), or a fine indicated in the person's license where higher.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Ghana's privacy laws are silent on tracking technology. Companies that use tracking technology would still be required to abide by the basic principles on data privacy as outlined in the Data Protection Act when processing data.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions are regulated by the Gaming Commission, which is created and regulated by Act 721, Gaming Act 2006 ('Gaming Act').

The Gaming Act sets guidelines for running promotional and loyalty programs in Ghana and categorizes those that need to be registered or not by the Gaming Commission before they can take place.

Under the Gaming Act, games of chance must be licensed by the Gaming Commission. However, games of chance incidental to certain entertainment, such as a fete or bazaar, and those promoted by a society if limited to its members, are exempted from the need for licenses as long as they comply with certain provisions.

Sanctions for the breach of the Gaming Act include various terms of imprisonment and fines ranging between 250 and 1,000 penalty units (approx GH¢ 3,000–12,000 (USD 194–774)).

7.4 How is social media and influencer marketing regulated under privacy law?

Ghana's privacy laws currently do not have provisions that specifically address privacy in respect of social media and influencer marketing. However, the Data Protection Act states that direct marketing includes communication by whatever means of any advertising or marketing material which is directed to particular individuals.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

The Electronic Communications Regulations provide that a person who wishes to send unsolicited communications for direct marketing by call, email or text message must first obtain the consent of the subscriber. The communication must include the name and contact details of the sender where it can be reached free of charge. Where the unsolicited communication is by means of an email, the sender must ensure that its identity is not concealed and must provide a valid address to which the subscriber can request the person to desist from sending such messages.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Our laws do not currently provide for digital identity resolution and clean room technologies. However, general data protection laws will apply to these technologies in relation to privacy.

7.7 How is location-based advertising regulated under privacy law?

Our laws do not currently provide specifically for location-based advertising. The provisions of the Data Protection Act, such as the prohibition on data controllers from using, obtaining, procuring, or providing information related to a data subject for direct marketing purposes without consent will also apply in instances of location-based advertising.

7.8 How are data brokers defined and regulated under privacy law?

The Data Protection Act does not specifically provide for data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

According to the Data Protection Act, a person must not process personal data which relates to a child who is under parental control in accordance with the law. For any data processing, including for advertising purposes, parental consent is required for minors.

Similarly, the AAG requires special care to be taken in advertisements directed at children or featuring children. These advertisements should not undermine positive social behavior, attitude, and lifestyle. Also, products suitable for children must be advertised in media targeted at them and advertisements directed at children must not be placed in media with editorial content unsuitable for children.

The Food and Drugs Authority ('FDA') and the Gaming Commission also have regulations dealing with advertising targeted at children such advertisements should not be misleading, exploit their vulnerability, or make drinking alcohol or gambling attractive to children or minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Ghana's privacy law does not explicitly regulate profiling or the use of artificial intelligence ('AI') or automated decision-making technology for advertising purposes. However, the provisions of the Data Protection Act in relation to obtaining consent and processing of personal data for marketing or advertising purposes will apply in this instance.

7.11 Are there other specific advertising practices that you wish to discuss?

In certain sectors, advertisements must be approved before they can be published or aired.

For instance, the FDA must approve advertisements related to food, drugs, cosmetics, household chemicals, and medical equipment before release to the public. Likewise, the Gaming Commission requires pre-approval for advertisements related to gaming and promotions.

Gaming advertising to children is prohibited and such advertising should not appear in media specifically aimed at children under 18 years, such as children's magazines or programs designed for young audiences. Furthermore, gaming advertisements, in particular, are prohibited from using children's songs or cartoon characters.

The FDA also prohibits advertising that exploits children's vulnerability or lack of experience. Advertising must not exploit fear, peer pressure, or other manipulative tactics to induce children to make purchases.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The Data Protection Act does not list countries where certain transfers are prohibited and requires all data controllers and data processors to comply with the provisions of the Act in relation to data privacy.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

- (a) The Data Protection Act prohibits the sale and purchase of personal data or information.
- (b) Personal data is exempt from the subject information provisions if it consists of information in respect of which a claim to professional privilege or confidentiality between client and a professional adviser could be maintained in legal proceedings.
- (c) There is an obligation on a data controller who processes personal data to ensure that the data is complete, accurate, and up to date. Also, such data should not be misleading in terms of the purpose for the collection or processing of personal data.
- (c) In relation to further processing of personal data, the Data Protection Act states that:
 - (i) such processing must only be for the specific purpose for which the data was collected;
 - (ii) a person who processes data must take into account:
 - the relationship between the purpose of the intended further processing and the purpose for which the data was collected,
 - the nature of the data concerned,
 - the manner in which the data has been collected,
 - the consequences that further processing is likely to have for the data subject, and
 - the contractual rights and obligations between the data subject and the person who processes the data; and
 - (iii) further processing of data is compatible with the purpose of collecting where:
 - the data subject consents to the further processing of the information,
 - the data is publicly available or has been made public by the person concerned.
- (d) Companies should be mindful of the above, as well as the need to notify data subjects and obtain their consent where needed before utilizing the data gathered.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Ghana? Are there minimum standards? Does this differ by sector or size of the entity?

A data controller must take the steps necessary to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organizational measures to prevent loss of, damage to, or unauthorized destruction, and unlawful access to or unauthorized processing of personal data.

Also, where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorized person, the data controller or a third party who processes data under the authority of the data controller must notify the DPC and the data subject of unauthorized access or acquisition and take steps to ensure the integrity of the information system is restored.

9.2 How are personal data breaches regulated in Ghana? What are the requirements for notification and response?

The data controller must notify the DPC and the data subject of the unauthorized access or acquisition, where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorized person, and take steps to ensure the restoration of the integrity of the information systems.

Upon confirmation that the data controller has breached any of the DPC's data protection principles, the DPC will serve the data controller with an enforcement notice requiring it to take steps or refrain from certain actions within specified timelines. The DPC may also require the data controller to refrain from processing personal data as specified in the notice or to refrain from processing personal data in a specified manner, or for specific purposes after the period specified in the notice, upon the confirmation of such breach.

A person who fails to register as a data controller, but processes personal information, commits an offence and will be liable, on conviction, to a fine of not more than 250 penalty units (approx GH¢ 3,000 (USD 193)) and/or a term of imprisonment of not more than two years.

The DPC must investigate and look into complaints made by data subjects against a data controller with respect to processing data, and, where applicable, direct the data controller to take steps to remedy the situation or desist from the acts complained of.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties for offences committed under the Data Protection Act include, amongst others:

- (a) for failing to register as a data controller but engaging in processing of personal data: a fine of not more than 250 penalty units (approx USD 193) and/or a term of imprisonment of 2 years;
- (b) for purchasing or knowingly obtaining or disclosing personal data to another person: a fine of not more than 250 penalty units (approx USD 193) and/or a term of imprisonment of 2 years;
- (c) for processing personal information of a child without complying with the provisions of the Data Protection Act, a fine of not more than 250 penalty units (approx USD 193) and/or a term of imprisonment of not more than 2 years;
- (d) for sale of personal data: a fine of not more than 2,500 units (approx USD 1,934) and/or a term of imprisonment of not more than 5 years; and
- (e) for all offenses for which the Act does not specify the penalty: a fine of not more than 5,000 penalty units (approx (USD 3,869) and/or a term of imprisonment of not more than 10 years.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under Ghanaian laws, consumers have the right to take legal action and seek various remedies if their privacy is violated. The legal framework blends both statutory laws and constitutional safeguards, some of which are outlined below:

- (a) The Constitution contains principles that recognize and protect the right to privacy of its citizens. In particular, it provides for the privacy of individuals and that this right should not be interfered with except in accordance with the law and for public safety, economic wellbeing of the country, health or moral reasons, or for the prevention of crime or protection of others.

The Constitution also provides that where the fundamental rights as provided for in the Constitution are breached, the affected person may approach the high court for redress.

- (b) The Data Protection Act states that ‘An individual shall at any time by notice in writing to a data controller require the data controller to cease or not begin processing for a specified purpose or in a specified manner, personal data which causes or is likely to cause unwarranted damage or distress to the individual.’ Where an individual suffers damage or distress through the contravention by a data controller of the requirements of the Act, that individual is entitled to compensation from the data controller for the damage or distress.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

- (a) The DPC is entitled to take certain steps where it is satisfied that a data controller has contravened or is contravening any of the data protection principles:
 - (i) The DPC shall serve the data controller with an enforcement notice to require the data controller to take steps or refrain from certain actions within specified timelines upon confirmation that the data controller has breached any of the DPC’s data protection principles.
 - (ii) The DPC may also require the data controller to refrain from processing personal data as specified in the notice or to refrain from processing personal data in a specified manner, or for specific purposes after the period specified in the notice, upon the confirmation of such breach.
 - (iii) The DPC also conducts periodic checks on companies in Ghana to ensure that they are complying with its data privacy rules. There have been instances where the DPC has arrested offenders with a view to prosecuting them in court.
- (b) There are also instances where private individuals have approached the courts to enforce their privacy rights in Ghana. One example is a 2024 unreported case, where the court found the defendants in breach of the privacy laws provided under the Data Protection Act and awarded damages in favor of the plaintiff. The court also mandated the DPC to ensure that the defendants and other similar ride hailing companies undertook liveness verification checks for riders, and audits to ensure that they comply with the privacy requirements of the Data Protection Act. This was to ensure that such companies upheld the obligations placed on them by law as data processors and to ensure the security, confidentiality, and accuracy of personal information and data being processed in Ghana.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Ghana?

We are not aware that any such rules exist at this time.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

In Ghana, advertising is currently regulated through a combination of sector-specific laws and guidelines; thus, the campaign for a single law which regulates advertising is still being promoted. The Bill proposed for the regulation of advertising and to establish the Advertising Council of Ghana is yet to be passed. The Bill is currently before Parliament. Once passed, it will be the major law regulating advertising in Ghana. The Bill is being actively promoted by the AAG.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Personal data processed by an individual for personal, family, or household purposes is not subject to the data protection principles. Similarly, personal data provided in confidence by a data controller for purposes such as education, training, employment, or appointment to a position, or for the provision of services by the data subject, is also exempt.

The provisions of the Data Protection Act do not apply when personal data is processed for purposes related to public order, safety, morality, or national security. Additionally, the Act does not cover personal data processing related to protecting the public from financial losses, malpractice in banking, insurance, investment, or other financial services, or dishonesty in professional services. It also does not apply when personal data processing is necessary for functions conferred by law on the government or Parliament, or for healthcare, disease prevention, and similar purposes.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The Supreme Court, in the case of *Mark Darlington Osaе v Food and Drugs Authority and Attorney General*, recently upheld the FDA's guidelines banning well-known personalities/celebrities from featuring in alcoholic beverage advertising. The court stated that the FDA's directive was not excessive or unreasonable, but was of the opinion that the ban was intended to sanitize the industry and protect children, who are easily influenced by celebrities, rather than to discriminate against celebrities.

This decision ended the controversy surrounding the ban, introduced in 2016 in the FDA Guidelines for the Advertisement of Foods, that no well-known personality or professional shall be used in alcoholic beverage advertising.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

A major challenge will be securing data that has been gathered from hackers or unauthorized users, due to the advent of technology.

The adoption of advanced technologies like artificial intelligence ('AI') and cloud computing while presenting opportunities and innovation in data processing may also pose risks for businesses and companies in terms of privacy. Companies should be mindful that poorly managed technologies can lead to breaches or misuse of personal data which can result in breach of their obligations under the Data Protection Act and other related laws in Ghana.

12.3 What do you envision the privacy landscape will look like in five years?

Due to the advance of technology, there may be greater challenges in ensuring the security and privacy of persona data across the globe, and this may trigger changes in the regulations of privacy across the world to deal with such challenges.

Increased use of AI in data processing will put more people at risk of breaching data privacy rules. Thus, there is an urgent need to review the laws regulating privacy in Ghana to adequately cover for and address the evolving trends in data processing and management to ensure proper protection of data in Ghana.

 GUATEMALA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Guatemala.

Data privacy protection is based on the Constitution, under which the right to privacy is acknowledged. The Constitutional Court has issued decisions covering the right to privacy, interpreting the extension of such right. The Court has applied the principle to informed self-determination and access to databases in which personal information is contained.

As of March 2025, Guatemala lacks specific legislation on data privacy; no specific regulations have been codified detailing matters such as how data can be collected, legally processed, transferred and enforced. In addition, the provisions relating to 'data privacy' contained in the American Convention on Human Rights should also be considered as applicable, as the Convention is applicable in Guatemala under the Constitution.

1.2 What are the primary laws regulating privacy in Guatemala? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The Public Information Access Law (Decree 57-2008 of Congress), among other matters, covers personal data contained in public archives or records. It contains a specific chapter on 'Habeas Data', defining it as the guarantee that every person has to exercise the right to access information about themselves contained in public files, records, databases, or other forms of public records, including the purpose of such information, as well as its protection, correction, rectification, or updating. Additionally, it establishes obligations for responsible entities regarding personal data, such as adopting procedures to receive and respond to access and correction requests, managing personal data only when it is adequate, relevant, and not excessive, and ensuring the security and confidentiality of personal data. The Law applies to public entities or entities that manage public funds and/or have competence in public administration.
- (b) The Criminal Code (Decree 17-73 of Congress) provides that the following are offenses:
 - (i) deletion of databases;
 - (ii) creation of prohibited records;
 - (iii) unauthorized alteration of the information contained in public databases; and
 - (iv) unauthorized use of data.
- (c) The Banks and Financial Groups Law (Decree 19-2000 of Congress) regulates, in general, the formation, operations and activities of banks and financial groups. Within such law, it is forbidden for a creditor or collection agent to oppress, annoy or abuse in an insistent and repetitive manner any debtor on the collection of a debt. It prohibits:
 - (i) making any kind of communication regarding the collection of a debt on non-business days/hours;
 - (ii) making two or more communications per day on such a matter;
 - (iii) collecting the debt from any person other than the debtor itself or its guarantor;
 - (iv) posting notices regarding the debt on poles or places near the debtor's residence or place of work.

- (d) The Law on the Recognition of Electronic Communications and Signatures (Decree 47-2008 of Congress), establishes regulations to safeguard data protection and privacy, particularly in the context of electronic communications and signatures. It imposes responsibilities on Certification Service Providers ('CSP's), requiring them to ensure the protection, confidentiality, and appropriate use of the information provided by signatories. CSPs are permitted to process certificate holders' data only for maintaining a publicly accessible record of issued certificates. However, such data must not be used for other purposes and must be retained for at least ten years. In terms of online information and consumer protection, companies engaged in e-commerce must respect consumer interests and adhere to fair business practices. They must also provide clear, visible, accurate, and easily accessible information about themselves and the goods or services they offer, ensuring transparency and consumer trust in digital transactions.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In Guatemala, due to the lack of specific regulation in this area, businesses and companies pay little attention to privacy. Generally, they comply by implementing privacy policies and terms and conditions of use for their online platforms. However, as more companies engage in commercial activities with the European Union, they have been compelled to align their practices with GDPR standards.

Currently, no private entity or organization in Guatemala issues guidelines, codes of conduct or best practices on data privacy, leaving each company to adjust its practices as it deems appropriate.

1.4 How is privacy law enforced in Guatemala? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy is enforced through tribunals via constitutional actions; in particular the amparo action (constitutional relief action). Depending on the infringement, there are administrative, civil and criminal procedures that can be initiated. See question 10.2. There are no privacy regulators, either public or self-regulatory bodies.

Since the right to privacy is a human right, individuals can also seek legal support through the Human Rights Ombudsman, in order to obtain protection regarding personal data and privacy.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Guatemala?

All companies are subject to the privacy provisions contained in the Constitution and are subject to the jurisprudence that emanates from the Constitutional Court. Although the amparo is a personal action, principles stated by the Constitutional Court when interpreting the Constitution may be of general application.

As previously expressed, the lack of specific regulation has left companies to implement their own policies regarding data privacy; with employees as well as in relation to clients and the public in general.

2.2 Does privacy law in Guatemala apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Constitution, the law and jurisprudence apply territorially (that is, locally), and all apply to both national and non-national companies operating in Guatemala. As of March 2025, the collection, export, import, or processing of personal data of residents in Guatemala by companies outside the country is not under specific regulations or requirements and there is no requirement to appoint a local representative. However, such actions must comply with the Constitutional Court's decisions and with the provisions of the laws that provide certain data protection (see question 1.2).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Guatemala?

As stated before, Guatemala lacks a data privacy law; however, under the the Public Information Access Law, 'personal data' is defined as information concerning identified or identifiable natural persons. Additionally, the Constitutional Court has stated that 'personal data' should be considered as being all data that allows the identification a person and enables the determination of a person's identity (ie, anything from an identification number to, among others, physical, social, cultural, and economic characteristics of such person).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Again, this answer can be found in the Public Information Access Law, which defines 'sensitive personal data' as data referring to physical or moral characteristics, facts, or circumstances of private life, such as personal habits, racial or ethnic origin, ideologies, political opinions, religious beliefs, health status, sexual preference, moral standing, and family situation. Regarding minors, data can only be collected with the authorization of their parents or legal guardian/tutor.

The law classifies sensitive or highly personal data as confidential information, which may only be accessed by the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

In the absence of specific regulations concerning data protection and privacy, anonymized, pseudonymized, or de-identified data do not receive specific treatment under the Guatemalan legal framework. Given the lack of comprehensive legislation addressing these categories of data, there is no clear legal provision or established standards regarding their handling, processing, or protection. Consequently, organizations are not subject to any distinct legal obligations or responsibilities regarding the use of such data under current law, leaving them largely unregulated in terms of privacy protections.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Lack of a specific law limits reference to provisions referred to as ‘obligations’, and whilst Guatemala’s Public Information Access Law provides an exhaustive list of entities subject to its provisions, private companies are not explicitly included. However, they may be considered obligated entities if they have been granted the right to exploit state-owned assets through a permit, license, concession, or any other contractual arrangement.

The law imposes specific duties regarding personal data protection on those entities subject to its provisions. These duties include:

- (a) establishing procedures to receive and respond to requests for access and data correction;
- (b) complying with the principle of data minimization, meaning they may only process personal data that is adequate, relevant, and not excessive for the intended purpose; and
- (c) ensuring the security and confidentiality of personal data.

Additionally, the Constitutional Court has referred in past decisions to principles to be considered by any company for processing personal information, including advertising, namely:

- (d) obtaining the explicit consent of the data subject;
- (e) not commercializing the data without authorization from the data subject;
- (f) guaranteeing data subjects:
 - (i) the right to consult their data,
 - (ii) the right to correct their data, and
 - (iii) confidentiality, unless the data subject has given express authorization for the data to be used in specific ways.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No, due to the lack of a specific privacy law in the country, roles applicable to the processing of personal data are not defined. The recommendation is for companies to deal with the matter contractually, considering international best practices.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Due to the absence of a specific privacy law in Guatemala, there are no established legal provisions that define a lawful basis for the general processing and handling of personal data. However, the Public Information Access Law provides some level of regulation in this area. Entities subject to its provisions may only process personal data when it is adequate, relevant, and not excessive in relation to the purposes for which it was collected. Additionally, these entities are expressly forbidden from disclosing, distributing, or commercializing personal data contained within information systems developed in the course of their duties. The only exception to this prohibition is when the individual to whom the information pertains has provided explicit, written consent for such use.

Although these provisions impose certain data protection obligations on public entities, Guatemala lacks a comprehensive data protection framework applicable to private organizations or data

processing in the commercial sector. Consequently, there are no clear legal requirements ensuring transparency, accountability, or lawfulness in the collection and use of personal data by businesses and private entities.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

In the absence of a specific law on privacy and data protection, the Guatemalan legal framework does not impose any duty or obligation on companies regarding the information that must be included in their privacy notices when processing personal data for advertising purposes. However, in practice, most companies adhere to the principles governing data processing established in the EU General Data Protection Regulation ('GDPR').

Accordingly, privacy notices commonly specify:

- (a) how personal data will be processed,
- (b) the determined and explicit purposes of such processing,
- (c) the mechanisms available for data subjects to rectify or delete their information, and
- (d) the retention period for the collected data.

While not legally mandated, these practices align with international data protection standards and contribute to enhancing transparency and accountability in personal data processing so many organizations chose to follow them.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Based on the human rights of intimacy, dignity and honor, the Constitutional Court of Guatemala has established that the rights of individuals in relation to their personal data are:

- (a) the right to consult their data;
- (b) the right to correct their data;
- (c) the right to confidentiality of certain information from any unauthorized third party;
- (d) the right to have certain information excluded that may be considered extremely sensitive where it is the product of news or data that concerns only the individual concerned; and
- (e) the right that commercialization of their personal data be done only with their express and written consent.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

The Public Information Access Law establishes that obligated entities must obtain the express written consent of data subjects before disseminating, distributing, or commercializing personal data contained in information systems developed in the course of their functions.

However, due to the absence of a specific law on the matter in Guatemala, there are no established mechanisms or measures to ensure that companies obtain consent or provide individuals with the option to opt out of advertising activities. Nevertheless, in practice, many companies include unsubscribe buttons on their websites or newsletters, allowing users to remove themselves from automated mailing lists or similar marketing mechanisms.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

There are no specific privacy rules that govern the use of vendors and other third parties in advertising. In practice, it is recommended that companies follow the GDPR standards conducting due diligence on third-party vendors and have legally binding agreements outlining their responsibilities for data processing, security, and compliance. Additionally, it is advisable that companies provide clear and accessible privacy notices that disclose how third parties, including ad vendors, collect and process personal data.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

There is no specific regulation regarding this topic. Nevertheless, the Constitutional Court of Guatemala has ruled that the use of any personal data needs express consent from the data subject. Therefore, following on from this, the other principles also apply, meaning that all data subjects have the right:

- (a) to know the content of their personal data; and
- (b) to have guaranteed the right to consult and correct their data and the right of confidentiality in the customer matching process.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Due to the absence of specific regulations on this matter, companies are not currently expected to undertake due diligence measures. There are no established requirements regarding the conduct of impact assessments; therefore, companies are not obligated to carry them out.

At present, the only expectation placed on companies is to adopt the necessary measures to ensure the security—and, where applicable, confidentiality—of personal data, in order to prevent its alteration, loss, unauthorized transmission, or access.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications are not specifically regulated in Guatemala. Therefore, companies should observe the various regulations that are disseminated in different laws as well as the Constitutional Court decisions regarding data privacy as regards the content of communications and the way these are implemented. Also, although this is not currently a regulated practice, companies should at least consider that individuals should have the right to request the cessation of email marketing and push notifications.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies is not regulated in Guatemala. However, based on the decisions of the Constitutional Court, people are entitled to be informed as to how information and activity online is tracked, registered or controlled.

7.3 How are loyalty programs and promotions regulated under privacy law?

In Guatemala, the regulation of loyalty programs is primarily governed by the internal policies of companies, such as banks and retail stores. These policies typically outline the terms of participation, point accumulation, reward redemption, and the conditions under which membership may be suspended or canceled. There is currently no specific national legislation regulating these programs.

Promotions are regulated under the Consumer and User Protection Law; however, the legislation does not address privacy-related matters. It only requires that the terms and conditions of any promotion be clearly stated.

7.4 How is social media and influencer marketing regulated under privacy law?

In Guatemala, regulation of social networks and influencers is limited, but there is growing concern about their impact, especially in the political sphere and in the protection of minors. There is no specific law that directly regulates social networks or influencers, but there are rules that apply to content and advertising in general.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

This kind of advertising is not specifically regulated. Nevertheless, Constitutional Court decisions make it clear that giving users information and obtaining their consent is key. The main principles that companies should observe are:

- (a) to obtain explicit consent from the interested parties;
- (b) to not commercialize data without authorization from the data subject;
- (c) to guarantee to data subjects:
 - (i) the right to consult their data,
 - (ii) the right to correct their data, and
 - (iii) confidentiality, unless there is express authorization from the data subject for the data to be used in specific ways.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Guatemala does not have a specific, comprehensive privacy law that directly regulates digital identity resolution and clean room technologies. However, certain legal provisions may indirectly apply to these technologies under the Public Information Access Law and general constitutional principles regarding privacy and data protection.

Since Guatemalan law lacks a dedicated framework for personal data processing, there are no explicit requirements for companies engaged in identity resolution, such as obtaining user consent, limiting data usage, or ensuring data minimization. However, as stated before, the Public Information Access Law establishes that personal data can only be processed when they are 'adequate, relevant, and not excessive' concerning their purpose. This principle may be relevant to identity resolution techniques that involve collecting extensive datasets from different sources. Additionally, since clean room technologies often operate under anonymized or pseudonymized data models, companies using clean room technologies should ideally obtain explicit user consent to mitigate potential risks.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not specifically regulated under Guatemalan privacy law. Currently, Guatemala lacks a comprehensive data protection framework that addresses the collection, processing, and use of geolocation data for advertising purposes. As a result, there are no explicit legal requirements or restrictions governing how companies may collect or utilize individuals' location information for targeted advertising. In the absence of such regulation, practices related to location-based advertising are generally guided by companies' internal policies and, where applicable, general principles of consumer protection and consent.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific privacy rules that govern data brokers. However, the Constitutional Court of Guatemala has ruled in respect of this matter. Data brokers, in order to gather, disseminate and commercialize personal data, must observe the following:

- (a) The collection of any personal data needs to have a defined purpose, and it must be collected in a legal and voluntary manner from the data subject.
- (b) Express consent of the data subject is required for use of any personal data; such use needs to be compatible with the purpose for which the data was collected.
- (c) Adequate mechanisms of control must be in place for the data broker to:
 - (i) determine the veracity of the data;
 - (ii) be able to update the data under its sole responsibility; and
 - (iii) have the right to rectify the data.

7.9 How is advertising to children and minors regulated under privacy law?

In Guatemala, advertising targeted at minors is subject to specific regulations aimed at safeguarding minors' rights and promoting their well-being. These regulations are primarily focused on preventing content that could harm the physical or mental health of children or encourage unhealthy behaviors. However, due to the absence of a comprehensive data protection law, the Guatemalan legal framework does not currently include provisions specifically addressing children's privacy or the protection of their personal data.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Guatemala does not currently have a comprehensive data protection framework that addresses the practice of profiling, including the automated processing of personal data to evaluate or analyze aspects related to an individual's behavior, preferences, or interests. As such, there are no clear legal provisions requiring transparency, consent, or safeguards in the use of profiling techniques. In practice, companies rely on internal policies and general consumer protection principles, but there is no binding national regulation governing profiling activities.

7.11 Are there other specific advertising practices that you wish to discuss?

To date, there have been no relevant legislative or regulatory advancements in Guatemala specifically addressing advertising practices beyond the general provisions contained in consumer protection laws. The current legal framework does not provide specific guidance on emerging advertising techniques, such as influencer marketing, native advertising, or behavioral targeting. As a result, companies operating in the Guatemalan market typically rely on general principles of transparency, fairness, and consumer protection, as well as their own internal policies and industry best practices.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There are currently no specific restrictions on the transfer of personal data, whether outside the country or between group companies. The requirements applicable to data transfers are the same as those that data brokers or data recipients must observe. These include ensuring that the data is processed in accordance with applicable legal standards and Constitutional Court rulings (see, for example, question 7.8).

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Companies are required to comply with the obligations established by the Constitutional Court (see, for example, question 7.8). Additionally, entities transferring personal data must ensure—through appropriate safeguards, such as contractual agreements—that the receiving party processes the data in accordance with the same legal and regulatory limitations.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Guatemala? Are there minimum standards? Does this differ by sector or size of the entity?

Data security in Guatemala is not comprehensively regulated under a specific data protection law. Currently, there are no established minimum standards or sector-specific requirements that govern how personal data should be secured, nor are there differences based on the size or nature of the entity processing the data.

The most relevant legal provision on the matter is contained in the Public Information Access Law, which primarily applies to public entities. This provides that: ‘the obligated parties shall be responsible for personal data and, in relation to such data, must ... adopt the necessary measures to ensure the security and, if applicable, confidentiality or restricted access to personal data, and to prevent its alteration, loss, transmission, and unauthorized access.’ However, the law does not define or specify what constitutes these ‘necessary measures,’ leaving their interpretation and implementation open.

While the law is addressed to public institutions, it could be reasonably interpreted as establishing general principles applicable to any organization—public or private—that handles personal data. In practice, however, due to the lack of clear definitions or enforcement mechanisms, data security obligations remain vague and are inconsistently applied.

As a result, companies and organizations in Guatemala are generally left to determine their own internal policies and procedures for data protection, often relying on international standards or industry best practices when implementing data security measures.

9.2 How are personal data breaches regulated in Guatemala? What are the requirements for notification and response?

In Guatemala, personal data breaches are not specifically regulated under a comprehensive data protection framework. There are currently no legal provisions that establish formal requirements for

breach notification, response procedures, or timelines, either to affected individuals or to regulatory authorities.

The only relevant provision is found in Public Information Access Law, as discussed at question 9.1.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

In Guatemala, penalties related to personal data breaches and misuse are specified under both the Criminal Code and the Public Information Access Law. The following outlines the key offenses and corresponding penalties:

(a) **Criminal Code:**

- (i) Destruction of database: Penalty: Prison term of 6 months to 4 years and a fine of Q200–2,000 (approx USD 25.50–255).
- (ii) Creation of prohibited records: Penalty: Prison term of 6 months to 4 years and a fine of Q200–1,000 (approx USD 25.50–128).
- (iii) Unauthorized alteration of information in databases: Penalty: Prison term of 1 to 5 years and a fine of Q500–3,000 (approx USD 64–383).
- (iv) Unauthorized use of data: penalty: Prison term of 6 months to 2 years and a fine of Q200–1,000 (approx USD 25.50–128).
- (v) Slander: Penalty: Prison term of 2 to 5 years.

(b) **Public Information Access Law:**

- (i) Unauthorized commercialization of personal data: Penalty: Prison term of 5 to 8 years and a fine of Q50,000–10,000 (approx USD 6,370–12,739).
- (ii) Alteration or destruction of information in archives: Penalty: Prison term of 5 to 8 years and a fine of Q50,000–10,000 (approx USD 6,370–12,739).
- (iii) Unjustified retention of information: Penalty: Prison term of 1 to 3 years, disqualification for twice the prison term, and a fine of Q10,000–50,000 (approx USD 1,274.00–6,370).
- (iv) Disclosure of confidential information: Penalty: Prison term of 5 to 8 years, disqualification for twice the prison term, and a fine of Q50,000–10,000 (approx USD 6,370–12,739).

- (c) **Civil actions for damages:** In cases involving personal data matters, affected individuals can pursue civil actions for damages. However, they must provide appropriate evidence to support the claim, and the amount of damages will be determined based on this evidence.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, consumers in Guatemala have a private right of action to seek remedies when their personal data rights are infringed:

- (a) **Amparo action:** Affected individuals may file a constitutional amparo action as a means of protecting their fundamental rights. This remedy can be used to put an end to actions or omissions that violate constitutional guarantees, including those related to personal data protection.

- (b) **Criminal action:** Individuals may also initiate a criminal action under the Criminal Code and the Public Information Access Law, which penalize certain unlawful acts involving personal data, such as unauthorized access, data theft, or disclosure (see question 10.1).
- (c) **Civil action:** In addition, individuals have the option to bring a civil action to claim damages. This may arise either as a consequence of a criminal proceeding or independently. In both cases, the primary remedy available is monetary compensation for the harm caused.

10.3 **How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.**

Currently, the primary enforcer in privacy-related matters in Guatemala has been the Constitutional Court. The Court has consistently upheld the right to privacy and the concept of habeas data in its rulings. For instance, in case file 3552-2014, dated February 10, 2015, the Court emphasized that the act of collecting and selling personal data without the express consent of the data subjects violates fundamental rights such as privacy, informative self-determination, honor, and reputation. This ruling reinforced the constitutional protection of personal data and the necessity of obtaining consent before processing such data.

However, despite the Constitutional Court's involvement, there have not been any landmark cases specifically related to privacy violations concerning advertising. While privacy violations in advertising practices could potentially fall within the scope of privacy protections, there have been no significant enforcement actions or lawsuits directly addressing non-compliance in the advertising sector related to privacy laws. Therefore, while privacy enforcement exists, it has largely been reactive, with no substantial cases directly tied to advertising practices.

11 **EMERGING CONSIDERATIONS**

11.1 **Are there cultural considerations that impact privacy law or enforcement in Guatemala?**

At the moment, the decisions of the Constitutional Court are the only reliable rules that can be used as a reference in privacy matters. However, these decisions may be limited in their application, as they stem from amparo actions—constitutional relief processes—that address specific factual scenarios. As such, while they offer important jurisprudential guidance, they do not provide the comprehensive regulatory framework typically expected for consistent enforcement and legal certainty.

A further consequence of this under-regulated environment is the general lack of awareness among the Guatemalan population regarding their privacy rights—how these rights can be protected and what mechanisms are available to enforce them. The limited visibility of privacy as a public concern, combined with the absence of educational campaigns or institutional efforts to promote data literacy, has led to a scenario in which individuals often do not recognize when their rights have been infringed or how to seek redress.

Guatemala remains at an early stage in the development of a comprehensive privacy and data protection culture. However, there is growing awareness among key stakeholders, and we remain optimistic that Congress will enact a dedicated data protection law in the near future. Such a step would not only clarify obligations and rights but also help close the knowledge gap and empower individuals to actively protect their personal information in an increasingly digital society.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

One of the emerging legal challenges in Guatemala is the regulation of political advertising through social media influencers. In 2023, the Supreme Electoral Tribunal prohibited influencers from promoting political content, even if sponsored by political parties. This signals a broader trend toward increased scrutiny of digital advertising and may lead to further regulations impacting how companies engage with influencers and manage sponsored content.

Additionally, in the past couple of years, the regulation of social media content has remained a contentious issue. While some experts advocate for oversight to prevent misuse and protect individuals’ reputations, others warn that such measures could infringe upon constitutional rights, particularly the freedom of expression. This ongoing debate underscores the need for companies to stay informed about potential legislative developments that may impact digital advertising and content dissemination strategies.

Lastly, an emerging concern in Guatemala is the increasing threat of data breaches associated with cloud computing. As businesses and individuals increasingly rely on digital platforms and remote working, cybercriminals are exploiting technological vulnerabilities to access sensitive personal and financial information. This trend underscores the urgent need for companies to implement robust cybersecurity measures and stay informed about potential regulatory developments in data protection.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Lack of legislation does not imply freedom of action. In Guatemala, the absence of a comprehensive data protection law does not mean companies are free from responsibility when handling personal data. On the contrary, entities processing personal information are encouraged to act proactively and responsibly, adhering to international standards and ethical principles to mitigate legal and reputational risks.

As such, it is highly advisable for companies to implement clear privacy notices, provide sufficient and transparent information to data subjects, and obtain explicit, informed consent whenever personal data is collected, used, shared, or transferred. These steps help ensure proper documentation and accountability, and can serve as critical evidence of compliance in the event of an investigation or legal challenge.

Given the current regulatory vacuum, it is advisable that companies operating in Guatemala adopt best practices based on internationally recognized frameworks, such as the EU GDPR. Although not legally binding in Guatemala, the GDPR offers a comprehensive and well-structured model for privacy governance. Its principles—including lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability—can guide organizations in developing robust internal policies and procedures.

In addition, companies should establish internal training programs, contractual safeguards, and data security protocols to ensure that all employees and business partners understand their obligations regarding personal data. This is particularly important in sectors that handle sensitive information or rely on data transfers, whether domestically or internationally.

Ultimately, a proactive, risk-based approach to privacy management will not only enhance consumer trust, but also better prepare organizations for future regulation, as momentum grows toward the eventual enactment of a national data protection law in Guatemala.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Amid growing national concern regarding the use of personal data, widespread dissatisfaction with the overwhelming volume of digital advertising across platforms, and heightened fears of cyberattacks, Guatemalan users are becoming increasingly conscious of their privacy. This shift in public awareness has led individuals to scrutinize how they interact with digital platforms, the type of information they share, and the content they consume.

This emerging trend has drawn the attention of both national and international stakeholders to Guatemala's digital and privacy landscape. In response, efforts have been made within the legislative branch to address these issues. Notably, Legislative Initiative Bill 6103, which seeks the approval of the Comprehensive Law for the Protection of Personal Data Held by Third Parties, received a favorable opinion from the corresponding congressional committee on January 17, 2023. The initiative was discussed in its first reading on January 25, 2023, and in its second reading on February 1, 2023. However, it has not progressed further and remains pending additional discussion.

Additionally, Legislative Initiative Bill 6105, which proposes the approval of a General Data Protection Law, received a favorable opinion from the relevant committee on April 28, 2023. As of today, the initiative has not been brought to the floor for its first reading, and no updates on its status have been made public.

These legislative developments reflect a growing institutional recognition of the need to establish a robust regulatory framework for data protection in Guatemala, although progress remains slow and uncertain.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

In the absence of a comprehensive data protection law in Guatemala, companies must adopt a proactive approach to the management and safeguarding of personal data. This involves carefully monitoring how personal data is obtained, processed, stored, shared, and deleted, ensuring that all data handling practices are transparent, lawful, and in line with internationally recognized standards.

To bridge the regulatory gap, companies are advised to develop and implement internal policies, notices, and contractual provisions that reflect best practices in data protection. These should include clear consent mechanisms, data retention policies, and protocols for handling data subject rights, even if not expressly required by law.

Furthermore, when engaging third parties, whether service providers, partners, or other entities, companies must exercise due diligence to ensure that these external parties uphold the same standards of data protection and security. This includes reviewing and negotiating data processing agreements or confidentiality clauses that impose equivalent obligations for handling personal data. Failure to ensure such alignment may expose companies to liability and undermine efforts to maintain a consistent and secure data protection framework.

Ultimately, in a developing regulatory environment such as Guatemala's, responsible corporate governance in data matters is not only a legal safeguard but also a strategic advantage that builds trust with consumers, clients, and regulators alike.

12.3 What do you envision the privacy landscape will look like in five years?

Over the next five years, Guatemala's privacy landscape is likely to shift due to increasing public concern over personal data use, digital advertising saturation, and cyber threats. This growing awareness has prompted national and international attention, leading to legislative efforts like Initiatives 6103 and 6105, which propose comprehensive data protection laws but remain stalled in Congress.

Looking forward, we envision two possible outcomes. The Constitutional Court may issue an exhortative decision urging Congress to enact a dedicated data protection law, as it has done in other matters of constitutional importance. Alternatively, Congress itself may respond to domestic and international pressures and move forward with privacy-specific legislation. In either case, companies operating in Guatemala should anticipate a more structured legal environment for privacy in the coming years and begin aligning their practices with international standards, such as the GDPR, to ensure compliance and build user trust.

HONDURAS

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Honduras.

There is no specific law to regulate privacy for Honduras. Laws, such as the Consumer Protection Law, and some others regarding how government officials/institutions must handle information for clinical trials, industrial patents and other related matters, give a very small regulatory framework on the matter.

In practice, companies tend to apply international standards for data privacy as best they can, in order to be able to commercialize/operate in regional markets; however, these regulations are not enforced in Honduras. Nevertheless, the Constitution of the Republic of Honduras regulates the right to honor, intimacy and secrecy of communications.

1.2 What are the primary laws regulating privacy in Honduras? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The key law would be the Consumer Protection Law, which, very broadly, touches on how companies must manage the information given to them by consumers, if consumer databases are managed by a company.

The Financial System Law also briefly states that companies in the same group can freely share information about consumers/clients amongst their group companies.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In Honduras, there is no specific role that is contemplated in the applicable regulations; however, good practices provide compliance from a global point of view, avoiding any doubt in the event of non-compliance with regulations.

1.4 How is privacy law enforced in Honduras? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Direction for Consumer Protection Office, which is managed by the Honduran Economic Development Ministry, is the body where consumers can file complaints against companies for any mismanagement of information.

Some government agencies have internal regulations which set out what information is considered sensitive or private, the precautions that must be taken in order to protect such information, and the consequences of any breaches.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Honduras?

As the Consumer Protection Law is the main regulatory framework, all companies which sell products directly to end-consumers are subject to privacy law.

- 2.2 Does privacy law in Honduras apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?**

No.

3 PERSONAL DATA

- 3.1 How is personal data defined under privacy law in Honduras?**

The Consumer Protection Law briefly states that companies may not sell or use consumer information for financial purposes but can share databases with each other. There is no distinction between what information is sensitive and what is not.

- 3.2 What categories of personal data are considered sensitive, and how are they regulated differently?**

The Honduran regulatory framework does not make a distinction as to what can be considered sensitive information and what not.

- 3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?**

Since there is no specific regulation on data privacy and the Consumer Protection Law is the law that, to some extent, governs the privacy of data acquired by companies from their consumers, there is no applicable legislation on the matter. However, it could be established that the same criteria may apply to anonymized, pseudonymized or de-identified data as for general data, meaning that their foreseen transaction (for financial purposes) or sale of such data is prohibited.

4 COMPANY OBLIGATIONS

- 4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?**

Certain specific sectors are required to provide all required information, including private information, to their regulatory bodies. For example, financial institutions are obligated to provide any and all required information to the National Banking and Insurance Board.

Other than that, there are no specific principles that companies are required to follow. In practice, international standards of transparency and choice are used by regional and international companies that operate in the country.

- 4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

No.

- 4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

Due to the lack of legislation in Honduras regarding the privacy of data for individuals and legal entities, there is no actual requirement for a lawful basis for data collection. However, we are of the

opinion that personal information must always respect the right to honor and privacy—therefore, although it is not required by law, it would be good practice to obtain the consent of the individual.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Even though the legislation does not address this, it is derived from the very concept of privacy that the privacy notice shall establish that the shared information will only be used by the person to whom it is shared and will only be used for the purpose for which it was shared.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

According to Honduran law, consumers have the following privacy rights:

- (a) right to honor;
- (b) right to intimacy; and
- (c) right to secrecy of communications.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

There is no need for companies to obtain consent. It could be done for compliance purposes, but legally it is not necessary.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

There is no legislation that addresses the use of vendors and other third parties in advertising.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

There is no legislation that addresses the disclosing of personal data. According to the Constitution of the Republic of Honduras, the rights to the secrecy of communications and honor must be respected.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must assess the risks associated with processing personal data, verify that the third parties with whom they share the information—or even the company’s own employees—comply with privacy regulations, and implement security measures to protect the collected data. Impact assessments can be carried out when the company faces a new situation, such as the use of new technologies or large-scale processing.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications are not regulated from a privacy perspective. Financial system laws only regulate the time periods during which companies can contact clients.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies are not regulated from a privacy perspective.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions are not regulated from a privacy perspective.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing is not regulated from a privacy perspective.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising and behavioral advertising are not regulated from a privacy perspective.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

They are not regulated by the Honduran legislation; therefore, it is international legislation that applies, although these regulations are not enforced in Honduras.

7.7 How is location-based advertising regulated under privacy law?

It is not regulated by the Honduran legislation; therefore, it is international legislation that applies, although these regulations are not enforced in Honduras.

7.8 How are data brokers defined and regulated under privacy law?

The concept of data brokers is not regulated or defined in Honduras, and so there isn't a law that establishes their obligations or the sanctions which they may incur. However, it is implied that people who have access to personal information must abide by what the Constitution and the Law on Transparency and Access to Public Information establish, that the only person allowed to have access to the information is the person themselves or their legal representatives.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors is not regulated by the Honduran legislation; therefore, international legislation applies, although these regulations are not enforced in Honduras.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

These matters are not regulated by Honduran legislation; therefore, international legislation applies, although these regulations are not enforced in Honduras.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There are no regulations on data transfer outside the country.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Honduras? Are there minimum standards? Does this differ by sector or size of the entity?

A law has recently been approved to regulate data security in companies which offer an electronic/digital signature service. There are minimum technical requirements for companies who offer these services, which are reviewed from time to time by the Intellectual Property Office in Honduras.

9.2 How are personal data breaches regulated in Honduras? What are the requirements for notification and response?

Data breaches are not yet regulated.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

If a breach/leak of private information can be traced to a company, and this causes damage to the party whose information has been breached, the affected party can file civil and criminal charges.

If the breach is covered by the Consumer Protection Law, it is punishable by fines from USD 400 to USD 4,000,000, depending on the severity and recurrence of the breach.

10.2 Do consumers have a private right of action? What remedies are available to them?

Everyone has the right to access information about themselves or their assets in an expeditious and free manner, whether such information is contained in public or private databases, and has the right, if necessary, to update, rectify and/or amend it.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

There is a low risk of enforcement at this end. We do not have information about any enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Honduras?

Privacy is only beginning to be a subject of relevance in Honduras; thus, rules governing it stem from international practices and regulations rather than within the country.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

A bill for regulating data protection has been brought before Congress. This received a lot of attention in 2017, but this dwindled at the end of 2018. To date, the National Congress has shown no interest in elevating this Bill to legislative discussion.

Additionally, data security is becoming very important in Honduras because of electronic communications, signatures and online banking.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Bill in Congress for data protection uses the international minimum standards for privacy, which many local companies do not yet comply with. Many companies will need to get up to speed and meet the international minimum standards to avoid sanctions and penalties in the future.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Globalization and regional efforts have had a big impact. Companies are expecting to manage most of their business on online platforms, which will push them to require regulations on data security and how companies who provide cloud services must manage the information. We are already seeing this with the electronic signature regulation and implementation (see question 6.1).

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The adoption of a specific regulation in terms of privacy and data security.

12.3 What do you envision the privacy landscape will look like in five years?

The country will hopefully have a specific regulatory framework for privacy and data security, not only in advertising, but for consumers, patients, clients, etc.

 HONG KONG

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Hong Kong.

Privacy per se is not protected in Hong Kong, as there is no Hong Kong legislative instrument protecting privacy per se.

The right to privacy is, in theory, constitutionally protected under the Basic Law, the ‘mini-constitution’ of Hong Kong. There are, however, no precedents or case law in Hong Kong where the Basic Law (or any other constitutional instrument) has been directly enforced against non-state actors (such as corporates or private citizens). In a report published by the Law Reform Commission of Hong Kong in 2004, the Law Reform Commission acknowledges that the Bill of Rights Ordinance and the Basic Law only create ‘a cause of action for breach of privacy against the Government or a public authority’ and that ‘Hong Kong courts have thus far not recognized a legally enforceable right of privacy at common law’.

Personal data privacy is protected in Hong Kong under the Personal Data (Privacy) Ordinance (‘PDPO’). The Hong Kong Court of Appeal has, however, confirmed in *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* that the PDPO does NOT confer a general right to privacy.

The Court of England and Wales has, in the 2008 case of *Mosley v Group Newspapers Ltd*, arguably expanded upon the common law tort of breach of confidence to protect breach of privacy in a certain extent. A (privately enforceable) duty of confidence arises where there is a ‘reasonable expectation of privacy’ and the common tort of breach of confidence could apply where such ‘reasonable expectation of privacy’ is violated. This may possibly be taken as a persuasive authority for a similar action in the Hong Kong courts—something which has not yet happened.

In 2004, the Law Reform Commission of Hong Kong recommended the introduction of legislation to target ‘invasion of privacy’, but no legislative action was taken.

1.2 What are the primary laws regulating privacy in Hong Kong? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

There are no laws in Hong Kong regulating privacy per se. See question 1.1.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Whilst not catering for the advertisement industry per se, the Privacy Commissioner for Personal Data (‘PCPD’), as Hong Kong’s leading governmental official in enforcing the PDPO, has advocated for all companies to develop their own privacy management program, to help companies comply with the legal requirement of the PDPO. To that end, the PCPD has published the *Privacy Management Programme: A Best Practice Guide* to provide examples and recommendations of how a company can establish the three components of ‘Organizational Commitment’, ‘Program Controls’, and ‘Ongoing Assessment and Revision’, that form a privacy management program.

In relation to the advertising industry, industry associations such as the Hong Kong Advertisers Association and the Association of Accredited Advertising Agencies of Hong Kong have not released any practice guides or guidelines for their members in relation to privacy or data privacy, save that the

Association of Accredited Advertising Agencies has, in its Code of Practice, reminded its members to comply with the restrictions under the PDPO for use of personal data in direct marketing (see questions 5.1, 7.1 below).

1.4 How is privacy law enforced in Hong Kong? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

There is no statutory machinery to enforce privacy per se. Individuals who believe their privacy has been infringed will likely have to bring civil actions under the common law tort of breach of confidence (see question 1.1).

The offence of ‘doxxing’, ie disclosing personal data, without the data subject’s consent, with intent to cause harm or being reckless as to whether harm would, or would likely, be caused to the data subject or any member of their family, introduced under the Personal Data (Privacy) (Amendment) Ordinance 2021 (‘Amendment Ordinance’), carries its own enforcement powers and penalties. Note, however, the ‘anti-doxxing’ offence falls under personal data privacy law, and not privacy per se. See questions 10.1 and 11.3.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Hong Kong?

Neither companies nor individuals are subject to privacy law per se as there is no such privacy law. Please, however, refer to the discussion on breach of confidence in question 1.1.

2.2 Does privacy law in Hong Kong apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

There is no privacy law in Hong Kong which applies to companies outside Hong Kong. Please, however, refer to the discussion on breach of confidence in question 1.1.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Hong Kong?

The PDPO, which was enacted in 1996, is the first statutory law in Hong Kong aimed at protecting the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith. Case law in Hong Kong, such as *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data*, has determined that this Ordinance does not protect personal privacy as opposed to information privacy.

Pursuant to the PDPO, ‘personal data’ means any data (itself defined as any representation of information (including an expression of opinion) in any document and includes a personal identifier):

- (a) relating directly or indirectly to a living individual;
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- (c) in a form in which access to or processing of the data is practicable.

This definition is commonly interpreted to include the Hong Kong identity card number of a data subject, and is arguably extendible to such representations of information as biometric measurement such as iris or gait (walking posture). The health record of a patient will normally fall within the definition of ‘personal data’ and accordingly protected under the PDPO.

Note also that the Personal Data (Privacy) (Amendment) Ordinance 2021 (‘Amendment Ordinance’) introduced the offence of ‘doxxing’, ie disclosing personal data, without the data subject’s consent, with intent to cause harm or being reckless as to whether harm would, or would likely, be caused to the data subject or any member of their family. See questions 10.1 and 11.3.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

There is no concept of ‘sensitive data’ under the PDPO, which does not distinguish between sensitive or non-sensitive information.

However, the PCPD has issued various guidelines and codes of practice in respect of certain types of personal data, such as biometric data, identity card numbers, health, video, geo-location and financial data and data related to children, which should be subject to more specific/tougher restrictions. Hence one may say that certain types of data are in practice considered sensitive and subject to a higher degree of protection under the PDPO.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

If personal data held is anonymized to the extent that a data user (or anyone else) cannot directly or indirectly identify the individuals concerned, such data is no longer considered as personal data under the PDPO and hence the PDPO does not apply.

In 2014, the PCPD issued the non-binding *Guidance on Personal Data Erasure and Anonymization*, stating that anonymization could be used as an alternative to erasure of personal data and setting out recommendations/best practice for anonymization of personal data. In these guidelines, the PCPD qualifies data anonymizing as:

- (a) the removal of any identifying information of an individual from personal data, and
- (b) the data user not being able to re-establish the identity of any individual with other existing or future information on the individual.

In addition, the PCPD has recommended that data users should make commitments that they will not attempt to re-identify any individuals from anonymized data, or to use such information even if re-identification is possible.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Data users (see question 4.2) are required to comply with the six Data Protection Principles (‘DPPs’) set out in the PDPO:

- (a) DPP1 provides that personal data should be collected in a lawful and fair way for a purpose directly related to a function or activity of the data user. The data collected should be necessary and adequate and not excessive for the purpose.

- (b) DPP2 requires that the personal data collected must be accurate and not kept longer than necessary.
- (c) DPP3 requires the data to be used only for the purpose for which it was collected or a directly related purpose, unless the data subject has given express voluntary consent.
- (d) DPP4 requires data users to take all practicable steps to protect the personal data they hold against unauthorized or accidental access, processing, erasure, loss or use (see question 9.1(b)).
- (e) DPP5 requires that all practicable steps be taken to ensure that a person can ascertain a data user's policies and practices in relation to personal data.
- (f) DPP6 gives data subjects the right to request access to and correction of their personal data if inaccurate.

The PDPO is much less extensive in its requirements relating to personal data privacy than counterparts such as the EU GDPR. Accordingly, there is currently no requirement in Hong Kong to appoint a privacy officer, nor to register with the PCPD, nor to conduct risk impact assessments, although voluntary compliance with such precepts would likely merit commendation by the PCPD.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

In relation to personal data, the PDPO defines:

- (a) 'data user' as a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data;
- (b) 'data subject' as the individual who is the subject of the data; and
- (c) 'data processor' as a third party to whom all activities involving personal data are subcontracted by the data user.

Under the PDPO, there is no direct connection between the data subject and the data processor, and the PDPO does not directly regulate data processors.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The PDPO requires that the data user must enter into a contractual relationship with the data processor, requiring the data processor to observe all relevant aspects of the PDPO in the processing of the personal data by the data processor for and on behalf of the data user. In essence, a data user is liable for breaches of data processors it engages.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

According to the PCPD's *Guidance on Direct Marketing* note, data users who wish to use personal data for their own direct marketing purposes, must obtain prior consent from data subjects, and notify them to the following:

- (a) that the data user intends to use the individual's personal data for direct marketing;
- (b) that the data user may not so use the personal data unless the data subject has received the data subject's consent to the intended use;

- (c) the kind(s) of personal data to be used;
- (d) the class(es) of marketing subjects (ie, goods/services to be marketed) in relation to which the data is to be used; and
- (e) the response channel through which the individual may, without charge, communicate the individual's consent to the intended use.

Furthermore, if the consent was given orally, data users must also send a written confirmation to the data subject confirming the particulars of the consent received.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See question 4.1 as to the DPPs. In particular:

- (a) Under DPP3 where a data user wishes to use personal data for any purpose which is unrelated to the original purpose of data collection they must obtain the data subject's informed consent. This is related to DPP1, whereby personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user.
- (b) DPP5 requires that all practicable steps must be taken to ensure that a person can ascertain a data user's policies and practices in relation to personal data. This data principle is normally honored and observed by the publication by the data user of a personal information collection statement and a privacy policy statement.
- (c) A data subject is entitled to find out whether a data user holds personal data of that data subject and it is entitled to request access to the personal data within a reasonable time, at a fee that is not excessive, in a reasonable manner and in a form that is intelligible. If the request is refused, the data subject must be given reasons. If the data held by a data user is found to inaccurate, data subjects have the right to request correction of the inaccurate data within a reasonable time, at a fee that is not excessive and in a reasonable manner. If the request is refused, the data subject must be given reasons.
- (e) Data users must take all practicable steps to erase personal data that is no longer required for the purpose for which the personal data was given.

Furthermore, the provisions of the PDPO relating to direct marketing, and of the Unsolicited Electronic Messages Ordinance ('UEMO') relating to unsolicited commercial electronic messages, all apply (see question 7.5).

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

The PDPO provides that a data user must obtain a data subject's explicit prior consent in order to use their personal data for direct marketing purposes. If the consent has been given orally, the data user has 14 days from receiving the oral consent to send a written confirmation to the data subject confirming the date of the receipt of the oral consent, the permitted kind of personal data and the permitted class of marketing subjects and it is required that the use to be made by the data user must be consistent with the consent of the data subject.

Where the consent or written consent of the data subject is required for processing, it can be given by way of:

- (a) a general blanket consent by the data subject to the data user to the use of or the transfer of their personal data in respect of all kinds of personal data or all classes of marketing subjects as specified in the consent; or

- (b) an express selection of a choice by the data subject to provide consent to some or all in the categories of:
 - (i) the kinds of personal data held by the data user;
 - (ii) the classes of the full range of marketing subjects offered by the data user; and
 - (iii) the intended class of transferees for use of the personal data in direct marketing.

Silence does not constitute consent, but a data subject can refuse to give any consent.

A data subject has the right to require a data user to cease use of their personal data in direct marketing, irrespective of whether or not the data was obtained directly from the data subject and whether or not an earlier consent has been given by the data subject to the data user or a third person for such use. A data user must, without charge to a data subject, cease use of the personal data upon receipt of such notification.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Currently there are no legal provisions specifically addressing the use of vendors and other third parties in advertising. Note that such third parties would likely be treated as data processors under the PDPO, and data users engaging such data processors are required to ensure data processors' compliance of the PDPO through contractual or other means (see questions 4.2, 6.2).

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

A data user who intends to provide the personal data of a data subject to a third person for use by that third person in direct marketing must:

- (a) inform the data subject in writing of that intention and that it may not provide the data without the data subject's written consent;
- (b) provide the data subject with the following written information:
 - (i) confirmation that the data user is to provide the data for gain,
 - (ii) the kinds of personal data to be provided,
 - (iii) the classes of persons to which the personal data is to be provided, and
 - (iv) the classes of marketing subjects in relation to which the personal data is to be used; and
- (c) provide the data subject with a channel through which the data subject may communicate their consent in writing without charge.

Unless the data user has complied with these requirements and has received the written consent of the data subject (either generally or specific to the intended provision of the personal data), the data user cannot provide the data subject's personal data to a third party for use by that third party in direct marketing.

A data subject may, at any time, require the data user to cease to provide their personal data to any other person for use by that other person, and require the data user to notify any person to whom the data has been so provided to cease the use of the data in direct marketing.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

The PDPO (originally enacted in 1996) is much less extensive in its requirements relating to personal data privacy than the 2016 GDPR of the European Union. There is currently no legal requirement in Hong Kong to undertake due diligence measures such as conducting risk impact assessments, although voluntary compliance with such would likely merit commendation by the Commissioner.

The PCPD does note that by following the various best practice guides and adopting its model frameworks, as well as utilizing contract laws principles, a data user can illustrate that it has taken reasonable precautions and exercised all due diligence, which could serve as evidence against charges under the PDPO.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The PDPO requires that a data user intending to market goods/services through direct marketing means (making solicitations addressed to specific person, eg, sending mail, email or making telephone calls to specific persons (eg, by name) and not at large) must:

- (a) inform the data subject that:
 - (i) the data user has the intention of using their personal data for direct marketing,
 - (ii) it may not use the personal data without the data subject's consent; and
- (b) provide the data subject with details of:
 - (i) the kinds of personal data to be used in the direct marketing, and
 - (ii) the classes of marketing subjects,

This must be done in sufficient detail to enable a practicable access by the data subject to ascertain the goods, facilities or services to be marketed with a reasonable degree of certainty; and
- (c) provide the data subject with details of a channel through which the data subject may, without charge by the data user, communicate consent to the intended use of the personal data.

After the required notification to the data subject, the data user must obtain the voluntary, explicit consent (which can be oral) of the data subject to the detailed communicated intention of use of the personal data in all messages of direct marketing.

If the consent has been given orally, the data user has 14 days from receiving the oral consent to send a written confirmation to the data subject confirming the date of the receipt of the oral consent, the permitted kind of personal data and the permitted class of marketing subjects and it is required that the use to be made by the data user must be consistent with the consent of the data subject.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There is no specific regulation of tracking technologies from a privacy perspective. Also note that there is currently no specific criminal offence of 'stalking' in Hong Kong.

In terms of data privacy, in May 2017 the PCPD published a best practice guide entitled *Physical Tracking and Monitoring Through Electronic Devices* to highlight the risks of data privacy associated with tracking or monitoring through monitoring devices, and recommendation for manufacturers of electronic devices.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions are not directly defined or covered by any specific law in Hong Kong; but the provisions of the PDPO relating to direct marketing, and of the UEMO relating to unsolicited electronic messages, all apply.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media is not directly defined or covered by any specific dedicated law in Hong Kong, but the provisions of the PDPO relating to direct marketing would continue to apply.

Furthermore, as of August 2023, the PCPD has made Hong Kong a signatory to the Joint Statement on Data Scraping and the Protection of Privacy, a joint statement made by 17 data protection authorities around the world which addresses the issues of data scraping, particular from social media platforms that host publicly available data, by outlining key privacy risks associating with data scraping, and how both social media platforms and individuals can protect personal information from data scraping.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There is no specific regulation on targeted advertising and behavioral advertising in Hong Kong.

However, under some circumstances, targeted advertisement may be a form of direct marketing and thus may be governed by the PDPO (see question 7.1). Under the PDPO, a data subject may at any time require a data user to cease to use their personal data in direct marketing. Upon receipt of such notification a data user must, without charge to the data subject, cease to use the personal data concerned. Where the opt-out choice is expressed orally by the data subject, the data user must follow up to comply with the requirement.

While the PDPO regulates direct marketing by any means to a data subject, the UEMO, administered by the Communications Authority of the Government of the Hong Kong SAR, regulates the sending of commercial electronic messages with a Hong Kong link.

A ‘commercial electronic message’ is defined as a message sent to an electronic mail address whose purpose (or one of the purposes of which) is to advertise, promote or offer goods, services, investment opportunities, or the supplier or provider of goods, services or investment opportunities.

There is a ‘Hong Kong link’ if the message originates in Hong Kong, is sent to Hong Kong, is sent to a Hong Kong telephone or fax number or a telecommunications device in Hong Kong that is used to access the message or an electronic address that is allocated or assigned by the Communications Authority. The restriction of the definition to a Hong Kong link recognizes the impossibility of including coverage and application to email sent to an overseas address because there is no international protocol for dealing with such messages.

The UEMO is technology-neutral and covers all types of commercial electronic messages, irrespective of the technology used by the senders. If the message is an email, all sender information should be prominently displayed either at the top, or at the bottom, of the body of the email message and be reasonably visible in terms of the font size, position and contrast/color.

The sender of an electronic message with a Hong Kong link is required to obtain the consent of the addressee, which may be given and withdrawn by means of an electronic message or in any other manner. Moreover, no person may acquire, supply, offer to supply or use address-harvesting software

or a harvested address list (or the right to use such software or list) for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link, without the consent of the registered user of the electronic address to which they are sent.

A person to whom an unsubscribe request is sent must ensure that a record of the request is retained in the format in which it was originally received for at least three years after the request. A commercial electronic message must not be sent after the date on which an unsubscribe request is sent. Nor may a commercial electronic message with a Hong Kong link be sent to an electronic address that, at the time the message is sent, is listed in a Do-Not-Call Register. The purpose of the Do-Not-Call Register is to provide:

- (a) registered users of electronic addresses with a convenient means by which they may notify senders of commercial electronic messages that they do not wish to receive such messages at those electronic addresses; and
- (b) senders of commercial electronic messages with a convenient means by which they may ascertain whether a registered user of an electronic address does not wish to receive unsolicited commercial electronic messages at that electronic address.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Currently there is no legal provision in Hong Kong relating specifically to digital identity resolution and clean room technology.

7.7 How is location-based advertising regulated under privacy law?

Currently, location-based advertising is not regulated under privacy law/data privacy law in Hong Kong.

7.8 How are data brokers defined and regulated under privacy law?

There are no privacy rules in Hong Kong governing data brokers except the provisions of PDPO requiring the consent of the data subject to the provision by the data user of the data subject's personal data to a third party for use by that third person in direct marketing (as to which see question 7.1).

7.9 How is advertising to children and minors regulated under privacy law?

DDP3 specifically states that the guardian/parent of a minor can give the consent required for the purpose of use of a minor's personal data for a new purpose; but, other than that, the PDPO has no provisions specific to children/minors. Nor does it prescribe different standards in protecting personal data of children/minors. Therefore, advertising regulations under privacy law, as covered in other sections of chapter, will apply to children as well.

That said, the PCPD, in a 2015 circular entitled *Collection and Use of Personal Data through the Internet—Points to Note for Data Users Targeting at Children*, does acknowledge that children are often identified as a vulnerable group. As best practice, data users should consider:

- (a) preparing age-appropriate versions of their privacy policies, including communications in gaining consent; and
- (b) providing a single dashboard on their online platforms for children to find out what personal data has been collected or used, change or remove personal data, and/or allow for parental controls to help children maintain their own personal data privacy.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Currently there are no provisions relating specifically to artificial intelligence or automated decision-making technology for advertising purposes. However, see question 11.3 as to AI generally.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There are no restrictions imposed by statute on data transfer. The provision in the PDPO on the prohibition on transfer of personal data to places outside Hong Kong except in specified circumstances remains on the statute book but has never been brought into effect. There is also no immediate plan for the government to implement it. However, if a data transfer abroad constitutes a new purpose, then consent from the data user under DPP3 will be required.

The PDPC also offers a set of recommended model contractual clauses for companies to use in relation to cross-border transfer of personal data for two different scenarios of transfers:

- (a) from data user to data user, and
- (b) from data user to data processor.

Furthermore, the PCPD recommends that a transferor of data should have effective data transfer arrangements, control activities that involved unintended or unnecessary cross-border data flow, and keep an inventory of transferred personal data. Note, however, the recommended model clauses are not binding requirements.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

If transfer of data was the intended purpose when the data was originally collected, or is the purpose of an extended use of collected personal data, then the consent of the data subject must be obtained.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Hong Kong? Are there minimum standards? Does this differ by sector or size of the entity?

Under DPP2, all practicable steps must be taken by the data user to ensure that personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used. All practicable steps must be taken to ensure that the personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is, or is to be, used and, as stated in question 6.2, where the data user engages a data processor, whether inside or outside Hong Kong, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

For these purposes, ‘data processor’ means a person who processes personal data on behalf of another person and does not process the data for any of their own purposes.

DPP4 requires that the data user take all practicable steps to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use, having particularly regard to:

- (a) the kind of data,
- (b) the physical location of storage of the data,
- (c) security measures incorporated into any equipment of storage of the data, and
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data and any measures taken for ensuring the secure transmission of the data

Where a data user engages a data processor, whether within or outside Hong Kong, to process personal data on its behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data which is transferred to the data processor for processing.

9.2 How are personal data breaches regulated in Hong Kong? What are the requirements for notification and response?

There are no specific provisions dealing with data breaches under the PDPO. There is no statutory reporting requirement (either to data subjects or the authorities) for data breaches. Data breach reporting is entirely voluntary.

However, the PDPC published the non-binding *Guidance on Data Breach Handling and Data Breach Notifications*, specifying that data breaches may amount to a contravention of DPP4 and recommending data users to establish a comprehensive data breach response plan to ‘help ensure a quick response to and effective management of a data breach’. The PDPC suggests that the response plan contain the following steps:

- (a) Step 1: Immediate gathering of essential information;
- (b) Step 2: Containing the data breach;
- (c) Step 3: Assessing the risk of harm;
- (d) Step 4: Considering giving data breach notifications; and
- (e) Step 5: Documenting the breach.

For Step 4, the PDPC recommends that in general, the data user should notify the PDPC and the affected data subjects ‘as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to those affected data subjects’ but falls short of mandating a notification requirement.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) Where no specific offence applies, if a data user has contravened one or more of the DPPs, the PCPD may issue an enforcement notice, requiring the data user to take steps to rectify the matter. A data user who contravenes an enforcement notice commits an offence and is liable to a fine of up to HKD 50,000 (approx USD 6,400) and to imprisonment for up to two years.

- (b) Specific offenses for non-compliance with the PDPO have a maximum penalty of a fine of HKD 500,000 (approx USD 64,000) and imprisonment for 3 years, or a fine of HKD 1 million and imprisonment of up to 5 years for more serious offences.
- (c) Knowing contravention of prohibitions in the UEMO carry a maximum penalty of a fine of HKD 1 million and 5 years imprisonment.
- (d) The Amendment Ordinance provides for the new specific offense of ‘doxxing’. It empowers the PCPD to demand the cessation of doxxing contents. These powers extend even to have an extra-territorial effect, so that a cessation notice may be served by the PDPC regardless of whether the disclosure is made in Hong Kong, and may be served on a Hong Kong person or, in relation to an electronic message, a non-Hong Kong service provider (eg operators of overseas social media platforms).
The offence of doxxing carries a penalty of a fine of HKD 100,000 and/or imprisonment for 2 years. Where the offence results in actual specified harm, the penalty rises to HKD 1 million and/or imprisonment for 5 years. See further question 11.3.

10.2 Do consumers have a private right of action? What remedies are available to them?

As stated in question 10.1, breaches of the statutory requirements of the PDPO (including the ‘anti-doxxing’ provisions) or of the UEMO are criminal offenses and attract fines and jail sentences. These provisions however do not confer private rights of actions to individuals.

Individuals seeking compensation for invasion of privacy will likely need to rely on the common law tort for breach of confidence (see question 1.1). Remedies include compensatory damages, exemplary damages and injunctive relief.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

As mentioned, there is no privacy law per se in Hong Kong.

The PCPD is moderately active in investigating personal data-related matters. The PCPD regularly conducts investigations and publishes investigation/inspection reports on personal data-related incidents, such as data breaches and personal data misuse complaints. Some of the subject matter investigated by the PCPD involving advertising include:

- (a) Unfair data collection, such as the placing of blind recruitment ads on online recruitment platforms to collect personal data of job applicants;
- (b) Collection of excessive personal data in marketing campaigns (such as loyalty programs);
- (c) Unauthorized collection or transfer of customer data for direct marketing purposes;
- (d) Sharing of clients’ personal data by different brands under the same company group;
- (e) Ransomware attack/data breaches of companies’ customer database.

Note that most enforcement actions are resolved by way of the PCPD issuing enforcement notices on the offending parties directing them to cease infringing acts and/or conduct remedial actions. Criminal enforcement for contravention of the PDPO (other than for doxxing offences) is rare.

For example, an enforcement report was published by the PCPD in December 2024, whereby a local online job recruitment platform, JobsDB, was found to have controlled the collection, holding, and processing of applicants’ personal data when they applied for a job advertised on JobsDB; and allowed recruiting organizations to publish advertisements on JobsDB as ‘Private Advertisers’ without disclosing their names, which made the advertisement ‘Blind Ads’.

The PCPD determined that both JobsDB and the ‘Private Advertisers’ were ‘data users’ and should have complied with the relevant requirements under the PDPO and the DPPs; and that both JobsDB and the ‘Private Advertisers’ were involved in the unfair collection of personal data of job applicants, and thus contravened DPP1(2).

The PCPD therefore served enforcement notices on JobsDB and three of the ‘Private Advertisers’ to take measures to remedy these contraventions and prevent recurrence of similar contraventions, while the remaining five ‘Private Advertisers’ were issued advisory letters instead.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Hong Kong?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) Anti-doxxing laws (see question 11.3);
- (b) Use of AI (see question 7.10).

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

- (a) **Doxxing:** The Amendment Ordinance was enacted in 2021 to amend the PDPO and to create criminal offences to curb acts of ‘doxxing’ which were becoming an increasingly severe infringement of personal data privacy. The government considered that doxxing had become prevalent in the second half of 2019, whereby members of the public took action to circulate, largely through social media and the Internet, personal data details of serving police officers, their wives and their children, such as their Hong Kong identity card numbers, personal addresses, email addresses and telephone numbers.

At the time, there was no express sanction or prohibition on such activities and so, in order to curb this flagrant and frequently very damaging exposure of personal data privacy details, the Amendment Ordinance was enacted.

The Amendment Ordinance has created two offences:

- (i) a summary offence for disclosing any personal data of a data subject without their relevant consent, where the disclosure is made with the intent to cause specified harm, or is reckless as to whether any specified harm would be, or would likely to be, caused, to the data subject or to any family member of the data subject.
- (ii) an indictable offence where the disclosure causes specified harm to the data subject or any family member of the data subject.

‘Specified harm’ is defined as ‘harassment, molestation, pestering, threat or intimidation to the person; bodily harm or psychological harm to the person; harm causing the person reasonably to be concerned for the person’s safety or well-being; or damage to the property of the person.’

It is notable that these new offences create protection not only of data subjects but also of their family members.

The PCPD is empowered to carry out criminal investigations and institute prosecutions, with the additional statutory power to demand the cessation of doxxing contents. These powers extend even to have an extra-territorial effect, so that a cessation notice may be served by the PDPC regardless of whether the disclosure is made in Hong Kong, and may be served on a Hong Kong person (eg, an individual in Hong Kong or an internet service provider having a place of business in Hong Kong) or, in relation to an electronic message, a non-Hong Kong service provider (eg operators of overseas social media platforms).

The PDPC is further empowered to require materials and assistance from any person whom the PDPC reasonably suspects, in relation to a specified investigation, has, or may have possession or control of any material relevant to that investigation, or may otherwise be able to assist the PDPC in relation to that investigation. Such person may be required by written notice from the PDPC to provide any material in their possession or control or to attend before the PCPD at a specified time or place and answer any question which the PDPC reasonably believes to be relevant to the specified investigation.

It should also be noted that the anti-doxxing provisions have already been invoked and there are already convictions under the provisions, with some convicted sent to prison.

- (b) **Telemedicine:** There has been a growth in the use of the internet for virtual medical consultation, digital scan and imaging, and remote provision of medical services through medical devices, all popularly subsumed to fall under the label of ‘telemedicine’.

Although telemedicine services can now be provided over the internet, for Hong Kong consumers, they are only available under the Ethical Guidelines on Practice of Telemedicine published by the Medical Council of Hong Kong in December 2019. Pursuant to these guidelines, only doctors who are admitted medical practitioners in Hong Kong are entitled to practice telemedicine, always provided that they adhere to established principles and standards, and remain fully responsible, for:

- (i) ensuring privacy and security of records;
- (ii) the informed consent of the patient;
- (iii) safe prescribing of treatment for the patient; and
- (iv) any other possible key areas of medical practice.

It is further required by the Ethical Guidelines that the doctor must be satisfied that the patient is suitable for a telemedicine interaction, and that the care to be delivered by a telemedicine is of a standard which is reasonable in all the circumstances of the specific context.

In Hong Kong, the health record of a patient will normally fall within the definition of ‘personal data’ under the PDPO and accordingly protected under the PDPO. Moreover, any doctor as a data user seeking and receiving the health and personal data of a patient for storage in a medical device and database must adhere to the DPPs. Such records are also protected under the Electronic Health Record Sharing System Ordinance (Cap 625), which supports healthcare service organizations in both public and private sectors to access a patient’s electronic health records.

- (c) **AI:** To keep up with the technical developments associated with the rapid development of artificial intelligence (‘AI’), in August 2021 the PCPD issued *Guidance on the Ethical Development and Use of Artificial Intelligence*, and, in June 2024, it published *Artificial Intelligence: Model Personal Data Protection Framework*.

Both sets of guidelines aim to offer best practice guides as to management AI systems internally, such as:

- (i) establish organizational AI strategy and governance standards;
- (ii) conduct risk assessment and adopting risk-based management approaches with appropriate risk mitigation measures and human oversight;
- (iii) customize and test AI models while properly managing data to ensure security; and
- (iv) communicate with stakeholders to enhance transparency and trust.

However, it is more crucial that organizations adhere to the guidelines' '7 Ethical Principles for AI', namely:

- (1) **Accountability for organizations:** to assess and address the risk of AI and provide justification for organizational actions;
- (2) **Human oversight:** Where the level of human involvement should be proportionate to the risks and impact of using an AI system, and to allow for human intervention where the risk of using an AI system is high;
- (3) **Transparency and interpretability:** Organizations should disclose their use of AI and their relevant data privacy practices;
- (4) **Data Privacy:** Effective data governance to protect individual privacy;
- (5) **Fairness:** Individuals are entitled to be treated in a reasonably equal manner, without unjust bias or unlawful discrimination;
- (6) **Benefits of AI:** Benefits are to be provided to human beings, businesses and the wider community. Where the use of AI may harm stakeholders, measures should be taken to minimize the probability and severity of the harm; and
- (7) **Reliability, robustness and security:** Organizations should ensure that AI systems operate reliably as intended over their expected lifetime; they should be resilient to errors to prevent or minimize unintentional harm.

These principles are intended to complement the DPPs, and thus organizations engaged in AI should ensure adherence to both sets of principles

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There has been no substantive change in the privacy law landscape since this book was last published in 2022.

There has, however, been some development in relation to AI. The PCPD has, in 2021 and 2024, issued non-binding guidelines in relation to AI. However, the Hong Kong Government is not expected to pass significant legislation specifically legislate for AI regulation in the near future, and AI will largely continue to be regulated by existing laws such as the PDPO.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Many provisions of the EU GDPR are noted with appreciation in the Hong Kong community. The PDPO does not go as far as the GDPR in protection of personal data privacy, and the feeling is that legislation to implement certain aspects of the GDPR would be welcome and effective.

12.3 What do you envision the privacy landscape will look like in five years?

The position is likely to remain stable in its present format.

INDIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in India.

The Supreme Court of India recognized the right to privacy as a fundamental right in the case of *Justice KS Puttaswamy (Retd) and Anr vs Union of India and Ors*, on August 24, 2017. This landmark ruling recognized privacy as an integral part of the right to life and personal liberty under Article 21 of the Indian Constitution.

This laid the foundation for the Digital Personal Data Protection Act 2023 ('DPDP Act'), which seeks to regulate the processing of an individual's personal data. The Act balances an individual's right to protect their personal data with the need to process such data for lawful purposes and related or incidental matters.

The Act also established the Data Protection Board of India ('DPBI'), an adjudicatory body responsible for resolving disputes between data principals and data processing entities.

In addition, the Information Technology Act 2000 ('IT Act'), provides for compensation for failure to protect personal data and punishment for disclosure of information in breach of a lawful contract.

Together, these legal frameworks illustrate India's commitment to safeguarding personal privacy and lawfully governing the processing of personal data in the digital age.

1.2 What are the primary laws regulating privacy in India? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy in India is primarily regulated at the national level by overarching legislation, such as the DPDP Act and the IT Act:

- (a) Key provisions of the DPDP Act include:
 - (i) **Informed consent and transparency:** The DPDP Act requires data fiduciaries to obtain specific and informed consent from data principals for the processing of their personal data;
 - (ii) **Protection of personal data:** Data fiduciaries must implement reasonable security safeguards to protect personal data;
 - (iii) **Rights of data principals:** Data principals have the right to access, correct, and erase their data. Data principals may also withdraw their consent for data processing and nominate individuals to act on their behalf; and
 - (iv) **Protection of minors:** There are special provisions to protect the data of minors (under 18 years of age), prohibiting harmful practices such as tracking, behavioral monitoring, or targeted advertising.
- (b) The IT Act provides for compensation when a body corporate fails to protect data due to negligence in implementing and maintaining reasonable security practices and procedures, which results in wrongful loss or gain to any person.

The provisions of the IT Act are implemented in conjunction with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (as amended in 2023) ('IT Rules'), which regulate the collection, processing, handling, disclosure, etc of personal information by organizations.

- (c) Additionally, the Indian Contract Act 1872 provides a civil remedy in cases where there is a violation of contract in disclosing personal information without consent.
- (d) Sectoral regulations, including guidelines issued by the Telecom Regulatory Authority of India and the Reserve Bank of India, also safeguard consumers against unwanted communications and ensure the confidentiality of customer data.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation does play a role in privacy regulation. The Advertising Standards Council of India, incorporated in 1985, is the primary self-regulatory body in India. While its Code of Self-Regulation does not explicitly specify privacy regulation, it promotes ethical considerations concerning privacy, such as avoiding the misuse of personal information.

Under the IT Rules, the government can designate as many online gaming self-regulatory bodies as it considers necessary for the purpose of verifying whether an online real money game is permissible.

According to the IT Rules, all social media intermediaries and online gaming self-regulatory bodies must appoint a grievance officer. Moreover, a 'significant social media intermediary' (ie, a social media intermediary with more than 5 million registered users) must appoint:

- (a) a chief compliance officer responsible for ensuring compliance with the IT Act and IT Rules;
- (b) a nodal contact person for 24/7 coordination with law enforcement agencies and officers; as well as
- (c) a resident grievance officer.

The IT Rules also envisage a three-tier structure for addressing grievances related to publishers of news and current affairs content, as well as publishers of online curated content:

- (i) **Level I:** Self-regulation by the publishers;
- (ii) **Level II:** Self-regulation by the self-regulatory bodies of the publishers;
- (iii) **Level III:** Oversight mechanism by the central government.

1.4 How is privacy law enforced in India? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

- (a) The DPDP Act is the foundation of India's privacy regime. The DPDP created the DPBI as an adjudicatory authority to deal with disputes arising out of personal data breaches and for enforcing compliance with data protection requirements. The DPBI can order remedial actions, investigate breaches, and impose penalty on organizations found to be in contravention of the Act.
- (b) The IT Act specifies punishment for different cyber-crimes, such as unauthorized access and data breach. The Act authorizes authorities to investigate and prosecute electronic data misuse offenses.
- (c) Indian citizens also have the right to pursue judicial remedy in civil courts in the event of violation of their right to privacy. They can bring actions for damages or injunctions against individuals or organizations that illegally process or use their personal information. These private actions act as a deterrent against prospective violations and supplement regulatory enforcement.

- (d) Moreover, industry-specific regulators, such as the Telecom Regulatory Authority of India and the Reserve Bank of India, provide guidelines to maintain consumer privacy in their respective sectors. For example, the Telecom Regulatory Authority controls unsolicited commercial communications to shield consumers from invasive marketing tactics.
- (e) In addition, the Competition Commission of India has moved to tackle privacy issues from a competition law point of view. See question 10.3.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in India?

A company becomes subject to privacy law if it engages in the processing of personal data within India. Under the DPDP Act, a company becomes subject to privacy law if it engages in the processing of digital personal data within India. This includes both personal data collected in digital form and data initially collected non-digitally but subsequently digitized.

2.2 Does privacy law in India apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The DPDP Act applies to the processing of digital personal data within India, where the personal data is collected:

- (a) in digital form, or
- (b) in non-digital form and later digitized.

Additionally, the DPDP Act applies to the processing of digital personal data outside India if such processing is in connection with any activity related to offering of goods or services to data principals within the territory of India.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in India?

The DPDP Act defines ‘personal data’ as any data about an individual who is identifiable by or in relation to such data.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The DPDP Act does not expressly define ‘sensitive personal data’ and instead regulates all personal data in a uniform manner.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The DPDP Act does not define ‘anonymized’, ‘pseudonymized’ or ‘de-identified’ data. The Act focuses on ‘personal data’ (see question 3.1).

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Under the DPDP Act, the key obligations for companies include:

- (a) **Informed consent and transparency:** The DPDP Act requires data fiduciaries to obtain specific and informed consent from data principals for the processing of their personal data. Data fiduciaries are required to notify:
 - (i) an itemized list of personal data being collected,
 - (ii) the purpose for collection of such data, and
 - (iii) a clear mechanism for withdrawing consent at any time.
- (b) **Protection of personal data:** Data fiduciaries must implement reasonable security safeguards to protect personal data, such as encryption, access control, monitoring for unauthorized access, and data backups.
- (c) **Personal data of children and persons with disabilities:** Data fiduciaries are required to obtain verifiable consent from parents or legal guardians before processing the personal data of children or persons with disabilities.

The Act also enforces purpose limitation and data minimization.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Under the DPDP Act:

- (a) **'Data fiduciary'** is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data; and
- (b) **'Significant data fiduciary'** is defined as a data fiduciary or a class of data fiduciaries notified by the central government under the Act. They are defined on the basis of the following criteria:
 - (i) the volume and sensitivity of personal data processed;
 - (ii) risk to the rights of data principal;
 - (iii) potential impact on the sovereignty and integrity of India;
 - (iv) risk to electoral democracy;
 - (v) security of the State; and
 - (vi) public order.

Significant data fiduciaries are subject to additional obligations: see question 6.3(b).
- (c) **'Data processor'** is defined as any person who processes personal data on behalf of a data fiduciary.

Data fiduciaries have the main responsibility for adherence to the provisions of the Act, including the application of adequate technical and organizational measures in order to ensure data protection. They are also responsible for the activities of the data processors they hire, requiring strong contractual provisions to impose compliance.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The personal data of a data principal can be processed for a lawful purpose for which the data principal has given their consent; or for certain legitimate uses. The legitimate uses include:

- (a) **Compliance with legal obligations:** Processing required for compliance with any law or court order;
- (b) **State functions:** Processing for the state for the purpose of delivering services or benefits, issuing certifications, or licenses or in the interest of sovereignty and integrity of India or security of the State;
- (c) **Medical emergencies:** Processing in case of medical emergencies or public health emergencies; or
- (d) **Employment purposes:** Processing required for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a data principal who is an employee.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the DPDP Act, data fiduciaries are required to provide data principals with clear and comprehensive privacy notices. When processing personal data for advertisement purposes, these notices should include:

- (a) an itemized list of the personal data being processed and the purpose for which it is intended to be processed;
- (b) the process through which data principals can exercise their right to withdraw consent, as well as their right to access easily available grievance redressal mechanisms; and
- (c) the process for filing a complaint with the DPBI.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Under the DPDP Act, consumers (or 'data principals') are accorded certain rights related to their personal data. These rights are:

- (a) **Right to information:** data principals have the right to obtain information about processing of their personal data, including the purpose of processing, categories of personal data being processed, and information regarding any third parties with whom the data is shared;
- (b) **Right to correction and erasure:** a data principal has the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent; and
- (c) **Right to grievance redressal:** data principals are entitled to redressal of grievances on matters concerning the processing of their personal information.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the DPDP Act, organizations must obtain consent from individuals (data principals) before processing their personal data for advertisement purposes. Consent must be free, specific, informed, unconditional, and unambiguous, expressed through a clear affirmative action. For children's data (ie, individuals under 18 years of age), parental consent is required. Prohibited actions include tracking, behavioral monitoring, and targeted advertising aimed at children. A data principal also has the right to correct, complete, update, and erase their personal data that was previously processed with their consent.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The data fiduciary remains responsible for complying with the provisions of the DPDP Act, even when a third party is used. A data fiduciary can engage a third party only under a valid contract that outlines the responsibilities and obligations of the third party. The data fiduciary must implement appropriate technical and organizational measures to ensure the effective observance of the DPDP Act. The data fiduciary is responsible for ensuring that reasonable security safeguards are in place to prevent data breaches, including when personal data is processed by a third party. Upon the withdrawal of consent by the data principal or when the data is no longer required for the specified purpose, the data fiduciary must erase the personal data and ensure that the third party also erases any data that was provided for processing.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

In accordance with the DPDP Act, data fiduciaries must establish specific contractual terms when sharing personal data with third parties or vendors. These terms are designed to ensure compliance with data protection requirements and safeguard individuals' rights. Some of the key contractual obligations include:

- (a) **Clear instructions for processing:** Contracts should clearly outline the scope, nature, and purpose of data processing activities, including the types of personal data involved and the duration of processing. This ensures that data processors handle the data in strict compliance with the data fiduciary's directives.
- (b) **Implementation of security measures:** Data fiduciaries must require data processors to adopt appropriate technical and organizational measures to protect personal data from unauthorized access, loss, or breaches. This includes deploying robust cyber security measures and conducting regular assessments to maintain data integrity and confidentiality.
- (c) **Support for data principal rights:** Data processors are obligated to assist data fiduciaries in responding to data principals' requests to exercise their rights, such as access, correction, or erasure of personal data. This cooperation is essential for ensuring compliance with the provisions of the DPDP Act.
- (d) **Breach notification procedures:** Contracts should mandate that data processors promptly notify data fiduciaries in the event of a data breach. Timely notifications allow data fiduciaries to take appropriate action to mitigate risks and fulfill regulatory reporting obligations.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Under the DPDP Act:

- (a) A data fiduciary must implement appropriate technical and organizational measures to ensure compliance with the Act. It must protect personal data in its possession, including data processed by a data processor, by taking reasonable security measures to prevent breaches. The data fiduciary must also publish the business contact information of a DPO or a designated representative to address data principals' inquiries about data processing. Additionally, an effective grievance redressal mechanism must be established.
- (b) For significant data fiduciaries, the following measures apply:
 - (i) **Appointment of a DPO:** The DPO must be based in India, report to the Board, and serve as the point of contact for grievance redressal.
 - (ii) **Appointment of an independent data auditor:** The auditor will evaluate the data fiduciary's compliance with the Act.
 - (iii) **Other measures:** These include conducting periodic DPIAs, regular audits, and other prescribed measures consistent with the Act.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing via calls or texts have been regulated under the Telecom Commercial Communication Customer Preference Regulations 2018, wherein the Telecom Regulatory Authority of India strictly regulates unsolicited commercial messages, requiring businesses to register and obtain prior user consent before sending marketing communications.

Now, under the DPDP Act, personal data can only be processed with consent, including for marketing purposes. Users must be given a clear opt-in choice and the ability to opt out easily.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Under the DPDP Act, explicit user consent must be obtained to use cookies or other tracking technologies.

7.3 How are loyalty programs and promotions regulated under privacy law?

Under the DPDP Act, the IT Act, and the IT Rules, participants in loyalty programs and other promotions have the right to access, withdraw, correct, and, under certain circumstances, object to the collection or processing of their personal data. The sponsor/organizer must provide an email address and/or physical address for participants to exercise these rights. Additionally, the sponsor/organizer must disclose where the participant's personal data will be stored. Any third-party entities involved are required to sign confidentiality agreements and implement appropriate technical and organizational measures to protect personal data from unauthorized access, loss, or breaches.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media platforms must obtain explicit consent from users before collecting or processing their personal data.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Under the DPDP Act, targeted advertising, requires explicit user consent, as it involves processing personal data to track user behavior or preferences. Users must be informed about how their data will be used and have the right to opt out at any time. Further, tracking or behavioral monitoring of children or targeted advertising directed at children are prohibited under the Act. In contrast, contextual advertising is not regulated under the DPDP Act. This distinction means personalized ads face stricter compliance requirements, while contextual ads remain largely unrestricted.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Under the DPDP Act, any processing of personal data, including combining data for identity resolution or sharing in clean rooms, must be based on explicit and informed user consent. The Act enforces purpose limitation, data minimization, and requires anonymization for data sharing in clean rooms to avoid identification of individuals.

7.7 How is location-based advertising regulated under privacy law?

All the above provisions regarding personal data apply to the collection of location data as well, including the requirement for specific and informed consent, complete transparency about the data to be collected, its purpose, and whether it will be shared with third parties.

7.8 How are data brokers defined and regulated under privacy law?

Under the DPDP Act, there is no specific definition or mention of ‘data brokers’. Given the Act casts a wide net over personal data, it may be understood that data brokers should also abide by the principles of the Act: ie, obtain valid user consent, adhere to purpose limitation, ensure data minimization, and allow users to access, correct, and erase their data.

7.9 How is advertising to children and minors regulated under privacy law?

Under the DPDP Act, the data fiduciary must obtain verifiable parental consent before processing any personal data related to children. Behavioral monitoring of children or targeted advertising directed at children is prohibited.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Currently existing privacy laws do not specifically address profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes. However, it can be understood that if an AI is being trained on personal data, the provisions of the DPDP Act are applicable.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Under the DPDP Act, cross-border transfer of personal data is generally allowed except to any country or territory which might be excluded by official notifications from central government. Prior to cross-border transfers of personal data, Data fiduciaries have to adhere to certain requirements provided by central government.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Central government can limit the transfer of data to certain territories or countries through notifications. Organizations need to frequently check for any such notifications so that they comply. Significant data fiduciaries have the extra obligations of:

- (a) appointing a DPO who is located in India, and
- (b) performing data protection impact assessments.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in India? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is regulated in India by the IT Act, along with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 ('CERT-IN Rules') and the CERT-IN Directions. Entities must follow 'reasonable security practices and procedures', with ISO/IEC 27001 being the standard.

Different sectors such as finance, telecommunications, securities, insurance, etc, have their own data security rules, often stricter than the IT Act. There is no differentiation by size of the entity.

9.2 How are personal data breaches regulated in India? What are the requirements for notification and response?

Under the DPDP Act, if a personal data breach occurs, the data fiduciary must notify both the affected data principals and the DPBI. The draft DPDP Rules outline how this notification should be made, including the required content and timeframe. The DPDP Act defines a personal data breach broadly to include any unauthorized handling of personal data—such as accidental disclosure, access, sharing, modification, destruction, or loss—that affects its confidentiality, integrity, or availability. This means data fiduciaries must report all personal data breaches, regardless of their severity or impact.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The DPDP Act lists following categories of violations that can attract a penalty of up to a certain amount:

- (a) Failure to take reasonable security safeguards to protect them from breach: a fine of up to 250 Crore (ie, INR 2,500 million—approx USD 30 million);

- (b) Failure to give notice to the DPBI and affected individuals about a data breach: a fine of up to 200 Crore (approx USD 23 million);
- (c) Breach in obligations regarding processing children’s personal data: A fine of up to 200 Crore (approx USD 23 million);
- (d) Failure by entities designated as significant data fiduciaries to meet their additional responsibilities: a fine of up to 150 Crore (approx USD 18 million); and
- (e) Breach of other requirements specified in the DPDP Act: a fine of up to 50 Crore (approx USD 6 million).

Additionally, the Act imposes a penalty of up to INR 10,000 (approx USD 117) on data principals who provide false information or file frivolous complaints.

10.2 Do consumers have a private right of action? What remedies are available to them?

Indian citizens also have the right to pursue judicial remedy in civil courts in the event of violation of their right to privacy. They can bring actions for damages or injunctions against individuals or organizations that illegally process or use their personal information. These private actions act as a deterrent against prospective violations and supplement regulatory enforcement.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

While the DPDP Act has been passed in India, the rules made under it have not yet been finalized. As a result, there have been no examples of enforcement action or litigation under the DPDP Act. However, the Competition Commission of India has taken steps to address privacy issues from a competition law perspective. In November 2024, it fined Meta Platforms USD 25.4 million and ordered WhatsApp to stop sharing user information with other Meta companies for advertising purposes for five years, citing antitrust violations related to WhatsApp’s 2021 privacy policy.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Argentina?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

While the DPDP Act has been enacted in India, it cannot be implemented fully until the draft DPDP Rules 2025 are finalized and enforced. Therefore, uncertainty remains around breach reporting timelines, cross-border data transfers, obligations for significant data fiduciaries, and several other provisions.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

We believe all the relevant statutes and regulation have been covered in previous sections.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, India's privacy landscape has undergone a major shift with the introduction of the DPDP Act, replacing earlier draft bills and establishing a comprehensive framework for the collection, processing, and protection of personal data. This change was triggered by growing concerns over data misuse, high-profile breaches, and the need to align with global privacy standards like the GDPR.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenges companies face amid India's evolving privacy landscape include uncertainty around compliance requirements under the DPDP Act, especially with pending Rules on breach reporting, consent, and cross-border data transfers. Companies must also manage the cost and complexity of updating data systems, ensuring user consent mechanisms, and (if classified as significant data fiduciaries) appointing DPOs. Additionally, the risk of high penalties and regulatory scrutiny has increased.

12.3 What do you envision the privacy landscape will look like in five years?

In five years, India's privacy landscape will likely feature strict enforcement of the DPDP Act, with clear compliance standards, active oversight by the DPBI, and greater alignment with global data protection norms. Companies will be expected to maintain high data security standards, with increased accountability for user privacy.

ISRAEL

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Israel.

Privacy in Israel is governed by a combination of laws, regulations and orders. First and foremost, the Knesset, Israel's Parliament, is responsible for enacting laws, including laws relating to privacy. Accordingly, the Knesset enacted the Privacy Protection Law 1981 ('PPL'). The PPL empowers the Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, to set regulations and issue orders.

1.2 What are the primary laws regulating privacy in Israel? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The PPL is the primary law. The Minister of Justice, in accordance with its powers pursuant to the PPL, has made a number of regulations and orders, including, but not limited to:

- (a) the Privacy Protection (Information Security) Regulations 2017 ('Information Security Regulations'); and
- (b) the Privacy Protection (Transferring Information to Databases Outside Israel) Regulations 2001.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There are no primary self-regulating privacy bodies in Israel. As described above, the Knesset and the relevant ministers, and Knesset Committees, deal with regulation.

1.4 How is privacy law enforced in Israel? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Primarily, privacy law is enforced by the Israeli courts. Individuals who consider that their privacy has been infringed, may bring a civil action against the infringer before a court of law.

Extreme infringement of privacy rights may be subject to criminal law. In such cases, the State, via the Prosecutor's Office, will bring criminal proceedings against the infringer before a court of law.

The Database Registrar ('Registrar'), derived from the PPL, is responsible for the registration, enforcement and administration of computerized databases. The Database Registrar heads the Privacy Protection Authority, which is the Israeli regulatory and enforcing authority for personal digital information. The Authority is responsible for the protection of all personal information held in digital databases.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Israel?

Activity of a company in Israel makes it subject to privacy law.

2.2 Does privacy law in Israel apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The PPL can namely be divided into two parts, privacy protection and databases. The first part relates to the classic privacy protection tort—the part which forbids the infringing of another’s privacy. It is clear that this part of the PPL applies to all companies, including companies outside Israel. Hence, foreign companies, acting in Isarel, may not infringe the privacy rights of Israelis. There is no need to appoint a local representative.

The second part of the PPL relates to databases—namely the collecting, storing, transferring and handling of information/data. While it is clear that the classic privacy law applies to all companies, including companies outside Israel, it is not clear whether the second part of the PPL relates to companies outside Israel. In theory, according to the letter of the PPL, there is no distinction between Israeli and non-Israeli companies. Thus, one could argue that the PPL, including the database chapters, apply to both foreign and domestic companies.

However, this interpretation would cause unrealistic results. For example, foreign companies would be bound by both their local database laws and Israeli laws, resulting in both duality and contradiction between two sets of laws. It should be noted that the Israeli courts, given the task of legal interpretation, have not, as yet, ruled on this issue.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Israel?

Under the PPL, ‘personal information’ means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Under the PPL, there are two types of data:

- (a) ‘regular’ data; and
- (b) ‘sensitive data’, which includes personal information—ie information on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person—and information that the Minister of Justice has by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, determined is sensitive.

In comparison to ‘regular’ information, sensitive information demands additional care while handling/storing. Additionally, the public is usually restricted in its access to sensitive information.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

There are no particular sections in the PPL which mention anonymized, pseudonymized, or de-identified data. Neverthelss, taking all facts of each individual case into consideration, anonymized, pseudonymized, or de-identified data, may, under certain circumstances, amount to privacy infringement.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Companies, inter alia, need to define, within a 'definition document':
 - (i) the methods of gathering and the use of the data,
 - (ii) the objects of the data's use,
 - (iii) the risks involved, and
 - (iv) the appointment of a database manager and supervisor.
- (b) The information security supervisor (see question 4.2) must set security procedures, and ensure that only authorized individuals have access to the stored information. The Information Security Regulations define four types of databases:
 - (i) databases bound by the strictest security obligations;
 - (ii) databases with medium security obligations;
 - (iii) databases with basic security obligations; and
 - (iv) databases managed by an individual which are bound by relatively lenient obligations.
- (c) It should be noted that certain types of databases require registration at the Database Registry. According to the PPL, database owners, including companies, are obligated to register their databases if one of the following applies:
 - (i) the database contains information on more than 10,000 persons;
 - (ii) the database contains sensitive information;
 - (iii) the database includes information on persons, and the information was not delivered to this database by them, on their behalf, or with their consent;
 - (iv) the database belongs to a public body; or
 - (v) the database is used for direct-mailing services.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Under the PPL, the owner of a database is responsible for securing stored information/data. Under the Information Security Regulations, companies and individuals (with the exception of sole individuals managing databases or sole-owned companies) must appoint an information security supervisor. The Information Security Regulations define 'information security supervisor' and 'database manager'. A database manager is responsible for the information security supervisor, who must report to the database manager.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Under certain criteria, databases must be registered at the appropriate government body ('registered database'). Registered databases must have a purpose.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The following information must be included:

- (a) the legal obligation to provide the data;
- (b) the purpose of collecting data;
- (c) the identity of the data receivers.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

First and foremost, Israelis have a constitutional right to privacy under the Basic Law: Human Dignity and Liberty. Secondly, under the PPL, individuals have a right not to have their privacy infringed. These rights are absolute, irrespective of context.

Israeli courts have adopted the 'right of publicity' from countries such as the USA, and enforced these rights upon Israelis. Accordingly, one may not use, for profit, a person's image, voice, name and personal affairs. Hence, advertisers should obtain clear consent from any person appearing in their advertisements. When minors appear in advertisements, parental or guardian consent must be provided.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Marketing communications are regulated by the Israel Communications (Telecommunications and Broadcasting) Act 1982. Under this Act, it is prohibited to market via emails, texts, push notifications or automatic dialing without receiving unequivocal consent from the addressee prior to sending the communication. Accordingly, Israel is considered an 'opt in' country.

After Israelis have 'opted in', they have the unconditional right to 'opt out' by providing a simple notification demanding to opt out.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

N/A

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies must:

- (a) clearly state what the purpose for which they hold the personal data,
- (b) use the data for the purpose it was collected; and
- (c) when transferring data, do so in a manner that does not risk breach of privacy.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must appoint officers responsible for securing data and must follow strict procedures for securing data. The rules and procedures are quite meticulous and complex. As the sensitivity of the stored data increases, the demands and procedures increase.

See also question 4.1.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications are regulated by the Israel Communications (Telecommunications and Broadcasting) Act 1982. Under this Act, it is prohibited to market via emails, texts, push notifications or automatic dialing without receiving unequivocal consent from the addressee prior to sending the communication. Accordingly, Israel is considered an 'opt in' country.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The PPL states 'no person shall infringe the privacy of another without their consent'. Cookies, pixels and SDKs 'follow'/'trail' consumers: acts which are in breach of one's privacy. Accordingly, cookies, pixels and SDKs are all subject to the consumer's consent.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions make use of data relating to the consumer. Moreover, when joining a loyalty program, the company organizing the program will usually send marketing material to the consumer. In short, all loyalty programs/promotions, should be defined by a written contract, in which the consumer, *inter alia*, agrees to:

- (a) use of their data; and
- (b) receive notifications, promotional emails, texts, etc.

7.4 How is social media and influencer marketing regulated under privacy law?

Influencers sending their followers marketing material and using their followers' data must receive permission to do so. Additionally, influencers must make it clear that they are sending marketing material/advertisements, in contrast to sending an 'ordinary' social post.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising is addressed in the PPL. When targeting consumers based on their personal traits, the text/advertisement must clearly state so. Moreover, the text must inform the targeted individual that they have the right to delete or amend the relevant database. These duties are not imposed on contextual advertising.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

N/A

7.7 How is location-based advertising regulated under privacy law?

N/A

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are defined by the PPL as those who hold databases and provide data to others. Such brokers must:

- (a) register their database at the appropriate governmental authority;
- (b) disclose:
 - (i) the fact that they hold such databases, and
 - (ii) the purpose of the databases; and
- (c) hold lists which set out:
 - (i) the source of their data, and
 - (ii) to whom the data has been transferred.

7.9 How is advertising to children and minors regulated under privacy law?

In Israel, a 'minor' is defined as an individual under the age of 18. When seeking consent to use a minor's details, it is highly recommended to seek parental consent.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The PPL does not prohibit profiling.

The issue of artificial intelligence has not, as of yet, been addressed in the PPL or by the courts in privacy law-related cases.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The transfer of data is regulated in the Privacy Protection (Transferring Information to Databases Outside Israel) Regulations 2001.

Under these regulations, subject to qualifications, a person must not transfer, nor enable the transfer abroad of data from databases in Israel, unless the law of the country to which the data is transferred ensures a level of protection no lower than the level of protection of data provided for by Israeli Law. The following principles apply:

- (a) data must be gathered and processed in a legal and fair manner;
- (b) data must be held, used and delivered only for the purpose for which it was received;
- (c) data gathered must be accurate and up-to-date;
- (d) the right of inspection is reserved to the data subject; and
- (e) the obligation to take adequate security measures to protect data in databases is mandatory.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

N/A

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Israel? Are there minimum standards? Does this differ by sector or size of the entity?

The PPL can namely be divided into two parts, privacy protection and databases. The first part relates to the classic privacy protection tort—the part which forbids the infringing of another’s privacy.

The second part of the PPL relates to databases—namely the collecting, storing, transferring and handling of information/data. All database holders are responsible for securing the stored data. A holder of several databases must ensure that only authorized individuals have access to the database. A holder of five or more databases which require registration must annually file a report listing the databases they possess, verified by an affidavit stating that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the information security supervisor.

Banks, public bodies, holders of five or more registerable databases, insurance companies and credit evaluators, must appoint a qualified information security officer.

9.2 How are personal data breaches regulated in Israel? What are the requirements for notification and response?

Data breaches are primarily regulated by the Privacy Protection Regulations (Data Security) 2017. A database owner must compose a ‘database definition document’. This document must include the risks associated with handling the database and the methods of dealing with data breaches.

Additionally, companies must compose a ‘security procedure document’ which prescribes the methods of dealing with security breaches. Further, companies which handle sensitive information, inter alia, must inform the Registrar in the event of a serious data breach has occurred.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

An infringement of privacy may result in civil and/or criminal proceedings.

According the PPL, an infringement of privacy is considered a tort. A court may award a plaintiff NIS 50,000–100,000 (approx USD 14,500–29,000) without the need to prove actual damages.

In a severe privacy infringement, whereby the infringer acted intentionally, criminal proceeding may be brought against the infringer by the State. Such crime is punishable by a prison term of up to 5 years and a fine not exceeding NIS 50,000 (approx USD 14,500).

In addition to monetary compensation, infringements relating to databases and the registration and handling of information may result in a one-year prison term.

Further, in privacy actions, a court may order injunctions and make various orders, including publishing its rulings and destroying material which violates privacy.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers have a right of action against those who infringe their privacy rights. Consumers, via the courts, may obtain injunctions against the infringers. Thus as an example, consumers may obtain an injunction ordering the infringer to cease infringement or amend/delete information held in a database.

Additionally, consumers, if successful in a law suit, may obtain monetary relief.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Most privacy actions, are civil actions brought by individuals against those who infringed their privacy. These law suits usually result in compensation and injunctions against the infringers, ordering the infringer to cease the infringing actions. Compensation sums depend on the severity of the infringement, and fluctuate from case to case. Compensation varies between a few thousand shekel to NIS 100,000.

In severe privacy infringement, the State may bring criminal action against the infringer. If the court finds the defendant guilty, 1-year prison sentences are common.

The State is quite active in bringing criminal action against privacy infringers. Most cases involve unauthorized use of private data.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Israel?

Approximately 14% of Israelis are observant orthodox, who are sensitive to their exposure before the public. Accordingly, advertisers should take note of the above.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

The hot topics include taking photos of or mentioning IDF soldiers. Accordingly, it is prohibited to publish photos or naming IDF soldiers from the rank of private to colonel.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The Privacy Protection (Instructions Relating to Data Transferred to Israel from the European Economic Area) Regulations 2023, recently entered force in Israel. According to these regulations, Israeli database holders must take special care of data that originated in the European Economic Area.

Inter alia, the Israeli database holder must:

- (a) erase data which was obtained in breach of the law;
- (b) erase data which in breach of the law;
- (c) erase data that goes beyond the database's purpose;
- (d) operate an organizational mechanism with the purpose of ensuring that the database does not contain unnecessary data or data that does not coincide with the database's purpose;
- (e) where they have received data from the EEA which relates to an individual, inform the individual of:
 - (i) the database's identity, manager and contact details,
 - (ii) the purpose of the data's transfer,
 - (iii) the type of data, and
 - (iv) the right to delete erroneous data.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

In order to comply with the various privacy-related laws and regulations, which are quite complicated to say the least, companies will need to spend more energy, time and thought on the issue of privacy protection and the handling of information/data.

Companies will need to spend an increased and significant amount of their income on expert advice and privacy compliance officers within their organizations.

12.3 What do you envision the privacy landscape will look like in five years?

The General Data Protection Regulation ('GDPR') which entered force in the European Union, has drawn vast interest in Israel. Though Israel is a country that is relatively respectful of privacy rights, it is not at par with the European Union. One can expect changes in the local legislation which mimic the GDPR.

JAMAICA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Jamaica.

Privacy is regulated in Jamaica under the Data Protection Act 2020, which the Government of Jamaica has recently implemented as part of its privacy policy. The Act requires custodians of web-based databases to maintain a system of integrity through physical and logical security of technology. The Data Protection Act 2020, which was enacted on July 10, 2020, seeks to safeguard the privacy and personal information of Jamaicans. The Government provided a two-year transitional period to allow data controllers time to take the required steps necessary to ensure full compliance with the legislation.

The right to privacy is expressly contained in Jamaica's Constitution pursuant to the Charter of Fundamental Rights and Freedoms, which states that everyone has a right to:

- (a) protection of private and family life, and privacy of the home, and
- (b) protection of privacy of other property and of communication.

The Jamaican courts have strongly expressed the importance of an individual's right to privacy. In the case of *Julian J Robinson v The Attorney General of Jamaica*, the Supreme Court of Jamaica came to the conclusion that privacy is a foundational right that enhances all other human rights and is in an indispensable component of a free and democratic society. The court acknowledged that the right to privacy means that an individual has control over whether their information is shared and under what circumstances sharing takes place. Additionally, the court has emphasized that society must operate on the basis that individuals have the right to be left alone, to be anonymous as much as possible and to retain control over their home, body, mind, heart and soul.

The right to privacy is also referred to in the Copyright Act of 1993 (last amended 2015) in relation to photographs and films.

1.2 What are the primary laws regulating privacy in Jamaica? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The Jamaica Constitution, Charter of Fundamental Rights and Freedoms;
- (b) The Data Protection Act 2020;
- (c) The Copyright Act of 1993 (last amended 2015);
- (d) Interception of Communications Act 2002;
- (e) The Cyber Crimes Act 2015;
- (f) The Access to Information Act 2002; and
- (g) The old Official Secrets Act.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Jamaican Code of Advertising Practice, which is a self-regulatory code, makes reference to privacy in the context of requiring the consent of living subjects for the use of their images in advertising. Consent is not required where, in the Council's opinion, the reference or portrayal in question is not inconsistent with the subject's right to a reasonable degree of privacy and does not constitute an unjustifiable commercial exploitation of his fame or reputation.

1.4 How is privacy law enforced in Jamaica? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Prior to the enactment of the Data Protection Act 2020 there were no regulatory bodies specifically enforcing privacy laws in Jamaica. However, on December 1, 2021 (at the end of the two-year transitional period), the Office of the Information Commissioner ('OIC') was established and the first Information Commissioner appointed.

The role of the OIC is:

- (a) facilitating the registration of data controllers: the OIC is responsible for overseeing the registration of data controllers and maintaining the register;
- (b) monitoring compliance with the Act and its accompanying Regulations and encourage best practices among controllers;
- (c) advising the Minister as appropriate on any matter relating to the Act or otherwise for the protection of personal data;
- (d) informing the public about the operations of the Act, good practices and any other matters within the Commissioners functions; and
- (e) consulting with trade associations or other persons representing data controllers, data subjects or representatives thereof to prepare and disseminate guidelines to be adhered to as good practice. In keeping with this, the Commissioner may encourage trade associations to prepare and adhere to self-initiated guidelines, provided they are in keeping with the Act.

Each year, a data controller must submit a data protection impact assessment ('DPIA') to the OIC outlining all personal data in their control within the first 90 days of each calendar year. The DPIA must outline a detailed description of all personal data held and an assessment as to whether the processing is necessary and/or proportionate based on the purposes it was collected for. The DPIA must also provide an assessment of the risks to data subjects rights, as well as any measures in place to protect the personal data and response mechanisms in the event of a breach.

Where the Commissioner is of the view that a data controller has breached the Data Protection Standards (see question 4.1), the Commissioner may serve an enforcement notice requiring that the data controller take certain actions, refrain from processing any or specific personal data or refrain from processing personal data for a specified period.

The Data Protection Act 2020 provides for private actions on the part of data subjects whose rights under the Act are breached. Individuals may file a complaint with the OIC or pursue civil action against the offending party or parties.

Outside of the data protection framework, private actions may also be brought before the courts for breaches of an individual's constitutional right to privacy. Overall, while the OIC is the statutory body with primary oversight for enforcement, enforcement mechanisms are multi-layered in nature, with sector-specific guidelines and individual rights and actions.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Jamaica?

All companies operating in Jamaica are subject to the laws of Jamaica.

Moreover, the Data Protection Act 2020 expressly states that the objects of the Act are to 'define the general principles for the treatment of personal data relating to an individual; and provide for

transparent oversight therefor, that will enable the public and private sectors to strengthen the protection of personal data.’ Thus making private and public sector players (individuals and companies) clear stakeholders in the privacy regime.

2.2 Does privacy law in Jamaica apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Data Protection Act 2020 provides that ‘personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.’ The requirements for a territory to meet this level of protection include having regard to the international obligations of that State or territory, the nature of the personal data, the law in force in the State or territory in question, among other considerations.

The Data Protection Act 2020 also established the persons and entities to which the law applies and the requirements for handling of personal data. The Act applies to data controllers established in Jamaica, and also to a data controller who, though not established in Jamaica, processes the data of an individual who is in Jamaica and the processing activities are related to the offering of products or services to individuals in Jamaica, or the monitoring of the behavior of individuals within Jamaica.

The Act requires that any individual or entity not established in Jamaica that qualifies as a data controller must appoint a data controller representative established in Jamaica, ie, an individual who is ordinarily resident in Jamaica, an entity established and formed in Jamaica or a person who maintains a regular practice in Jamaica.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Jamaica?

‘Personal data’ is defined in the Data Protection Act 2020 as ‘information (however stored) relating to a living individual or an individual who has been deceased for less than 30 years, who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, the data controller; and any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect of that individual.’

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Data Protection Act 2020 defines ‘sensitive personal data’ as consisting of any of the following information in respect of a data subject:

- (a) genetic data or biometric data;
- (b) filiation, or racial or ethnic origin;
- (c) political opinions, philosophical beliefs, religious beliefs or other beliefs of a similar nature;
- (d) membership in any trade union;
- (e) physical or mental health or condition;
- (f) sex life; and
- (g) the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under the Data Protection Act 2020, appropriate technical and organizational measures, including pseudonymization and encryption of personal data, must be taken against unauthorized or unlawful processing and accidental loss, destruction of or damage to personal data.

Willful and unlawful breach of this pseudonymization or encryption is an offence which shall make an offender liable to be fined.

Truly anonymised data, from which an individual cannot be identified, is not treated as personal data as defined under the Act. However, pseudonymized data, where re-identification is possible, will still trigger the provisions of the Data Protection Act.

As a best practice, advertisers should avoid making misleading claims about data being ‘anonymised’ when it is in fact only ‘pseudonymised’. Pseudonymised data may be able to be linked back to an individual using additional information. Where an individual can be identified, the Data Protection Standards will apply.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

All data controllers are required to comply with the Data Protection Standards in relation to all personal data within their control. These Standards are:

- (a) Fairness and lawfulness: personal data must be obtained and processed fairly and lawfully (see, further, question 4.3);
- (b) Purpose limitation: personal data must be obtained for a specific and lawful purpose and must be processed only in a manner compatible with such purpose;
- (c) Data minimization: personal data must be adequate, relevant and limited to the purpose for which it is collected;
- (d) Accuracy: personal data must be accurate and up-to-date;
- (e) Storage limitation: personal data must not be kept for longer than is necessary;
- (f) Data subject rights: personal data must be processed in accordance with the rights of the data subject (see question 6.2);
- (g) Technical and organizational measures: personal data must be protected using appropriate technical and organizational measures so as to prevent unauthorized or unlawful processing or accidental loss or destruction;
- (h) Cross-border transfers: personal data must not be transferred outside Jamaica unless that country ensures an adequate level of protection. See question 8.1.

In addition:

- (i) Personal data must not be processed by any data controller unless the registration particulars of that data controller are included in the register held by the Information Commissioner. Failing to keep this register updated is an offence under the Act;
- (j) A data controller must appoint an appropriately qualified person to act as the data protection officer, responsible, in particular, for monitoring in an independent manner the data controller’s compliance with the provisions of the Data Protection Act 2020; and

- (k) A DPIA must be carried out by the data controller, who must submit a DPIA in respect of all data in their custody or control within 90 days of the end of the calendar year. In addition, the Information Commissioner may request a DPIA on behalf of an individual who is directly affected by processing of personal data by that data controller.

The Information Commissioner may issue assessment notices or information notices to determine whether a data controller is acting in compliance with the law.

Jamaican companies must also abide by the EU General Data Protection Regulation ('GDPR'), since its scope extends beyond the EU jurisdiction when the personal data of EU citizens, the primary beneficiaries of the law, is being processed.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

A 'data controller' is defined in the Data Protection Act 2020 as 'any person or public authority who, either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed, and where personal data are processed only for purposes which they are required under enactment to be processed, the person on whom the obligation to process the personal data is imposed by or under that enactment is for the purposes of this Act a data controller'. See also question 2.2.

A 'data processor' is defined as 'any person other than an employee of the data controller, who processes the data on behalf of the data controller'.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, the First Data Protection Standard (see question 4.1) provides that personal data must be processed 'fairly and lawfully' and therefore requires a lawful basis for the processing of personal data. Personal data cannot be processed in accordance with the First Standard unless one of the following conditions is met:

- (a) the data subject has provided consent for processing and has not withdrawn that consent;
- (b) the processing is necessary for the performance of a contract to which the data subject is a party or for taking steps with a view to entering a contract;
- (c) the processing is necessary to protect the vital interests of the data subject;
- (d) the processing is necessary for the administration of justice, by law or for any other function of a public nature exercised in the public interest;
- (e) the processing is necessary in pursuance of legitimate interests by the data controller or any third party with which the data is shared, unless the processing is likely to cause prejudice to the rights and freedoms or legitimate interests of the data subject; or
- (f) the data subject has published the personal data concerned.

Where a data controller intends to rely on legitimate interest as the lawful basis for processing, the data controller must make a written assessment that:

- identifies the legitimate interest being pursued or any third parties with whom the data are shared;
- state the rationale for the processing to be necessary for the purposes of that legitimate interest; and

- state the rationale for the processing not being prejudicial to the rights or interests on the data subject having regard (but not limited) to the nature and source of all legitimate interests involved, the impact of the processing on the rights and freedoms of the data subject and all additional safeguards that could be or have been applied by the data controller to prevent any undue impact of the processing.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Privacy notices should include information on how personal data is collected, used, and shared in accordance with the Data Protection Principles, as well as data subjects' rights.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) The Charter of Fundamental Rights and Freedoms provides for the right of everyone to:
 - (i) protection from search of the person and property;
 - (ii) respect for and protection of private and family life, and privacy of the home; and
 - (iii) protection of privacy of other property and of communication;
- (b) Under the Data Protection Act 2020, a data subject also has the following rights:
 - (i) right of access to their personal data;
 - (ii) right to prevent processing likely to cause damage or distress;
 - (iii) right to prevent processing for purposes of direct marketing;
 - (iv) rights in relation to automated decision-taking; and
 - (v) right to rectification of inaccuracies.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

The Data Protection Act 2020 provides that a data controller may not process the personal data of a data subject for the purpose of direct marketing without the consent of the data subject except in limited circumstances. See question 7.1.

Any consent required to be given, by a data subject, to the processing of personal data must be:

- (a) informed,
- (b) specific,
- (c) unequivocal, and
- (d) freely given.

This may include such expression of consent given by the legal personal representative of the data subject or by the parents or guardians of a data subject who is a minor.

An individual is entitled at any time, by notice given in writing to a data controller, to require the data controller not to, or to cease, or not to begin processing that individual's personal data for the purposes of direct marketing.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

By virtue of the Data Protection Act 2020, required consent for the processing of personal data must be an informed, specific, unequivocal, freely given, expression of will by which the data subject agrees to the processing of their personal data.

As to direct marketing see question 7.1.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies must ensure that there is a legitimate basis for sharing an individual's personal data with third parties. Where a company engages a data processor, the processing must be carried out under a contract in writing and be clear that the data is only to be processed on the documented instructions of the company. Likewise, the contract must require the data processor to comply with the obligations imposed on the data controller, including a requirement for the processor to implement appropriate technical and organizational measures.

Further, if the data is to be shared with a vendor or third party outside of Jamaica, the Eighth Data Protection Standard provides that the data must not be transferred unless the territory to which it is being transferred has an adequate level of protection for the data (see question 8.1). However, the Eighth Standard does not apply under specific circumstances see question 8.2).

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

All privacy policies and practices are expected to incorporate the Data Protection Standards (see question 4.1).

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Data Protection Act 2020 provides that a data controller may not process the personal data of a data subject for the purpose of direct marketing unless the data subject consents to the processing for that purpose.

There is an exception where:

- (a) the data subject is a customer of the data controller;
- (b) the data controller has obtained the contact details of the data subject in the context of the sale of any goods or services;
- (c) the marketing is for the data controller's own similar goods or services; and
- (d) the data subject has been given a reasonable opportunity to object, free of charge, to such use of their personal data both at the time the data was collected and on the occasion of each marketing communication.

As to consent, see question 5.3.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There are currently no regulations on tracking technologies.

7.3 How are loyalty programs and promotions regulated under privacy law?

Although not specifically mentioned under the Act, loyalty programs and promotions are regulated under the Data Protection Act, if they involve the collection and use of personal data. In keeping with the Data Protection Standards, there must be a lawful basis for processing. For loyalty programs and promotions, the most relevant bases include:

- (a) **consent**—which must be freely and expressly given prior to the collection of data, Further, the consumer must be fully aware of what data is being collected, how it will be used, whether it will be shared with third parties and how long it will be retained;
- (b) **the performance of a contract**—if the loyalty program forms part of a service agreement, then processing will be permitted but must still align with data minimization and purpose limitation standards; or
- (c) **legitimate interest**—while businesses may rely on legitimate interest, they must be able to clearly identify the legitimate interest being pursued and the rationale for processing (see question 4.3).

7.4 How is social media and influencer marketing regulated under privacy law?

The Cybercrime Act 2015 criminalizes the act of intentionally or recklessly using a computer to send to another person data which is obscene, constitutes a threat, or is menacing in nature.

Further, where personal data is collected and processed for the purposes of social media and influencer marketing, the Data Protection Standards will apply, and the rights of data subjects are to be preserved.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are currently no privacy regulations for targeted advertising and behavioral advertising.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Clean room technology is not explicitly regulated under the Data Protection Act 2020. However, the willful and unlawful breach of required pseudonymization or encryption data security measures (see question 3.3) is an offence under the Act.

The Data Protection Act 2020 contemplates digital identity resolution for prescribed purposes including legal proceedings, seeking legal advice, and archival and historical purposes.

7.7 How is location-based advertising regulated under privacy law?

The Data Protection Act 2020 applies to data controllers processing personal data of persons in Jamaica, offering products or services to persons in Jamaica or monitoring the behavior of persons in Jamaica.

While not explicitly regulated under any statute, any location-based advertising must still be carried out in accordance with the Data Protection Act. In keeping with the Standards, the public must be clear on what data is being collected and how it is being used. The location data must be collected only for

explicitly stated lawful purposes. Likewise, in keeping with data subjects' rights under the Act, they must have the ability to opt out of this type of processing.

7.8 How are data brokers defined and regulated under privacy law?

The Data Protection Act does not explicitly define 'data brokers'; however, data brokers are still likely to face regulation under the Act, given that they process personal data. A data broker must therefore comply with the provisions of the Act.

7.9 How is advertising to children and minors regulated under privacy law?

The Data Protection Act 2020 provides that any consent required to be given by a data subject to the processing of personal data includes any such expression of consent given by a parent or legal guardian of a minor data subject.

Aside from this, there are no specific privacy rules governing advertising to minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The Data Protection Act 2020 provides that an individual is entitled at any time, by notice in writing to the data controller, to require the data controller to ensure that no decision is based solely on the automatic processing of the data subject's personal data for the purpose of evaluating matters relating to the data subject (for example, the individual's performance at work, creditworthiness, reliability, or conduct).

A data controller who receives a notice shall, within 30 days after receiving the notice, give the individual in question a written statement specifying the steps that the data controller intends to take to comply with the notice. If, on the application of a data subject, the Commissioner is satisfied that a data controller has failed to comply with a notice, the Commissioner may order the data controller to reconsider the decision, or to take a new decision, that is not based solely on automatic processing.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Under the Data Protection Act 2020, the Eighth Data Protection Standard (see question 4.1) provides that data must not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

Regard shall be given to:

- (a) the nature of the personal data;
- (b) the State or territory of origin of the information contained in the data;
- (c) the State or territory of final destination of that information;

- (d) the purposes for which and the period during which the data are intended to be processed;
- (e) the law in force in the State or territory in question;
- (f) the international obligations of that State or territory;
- (g) any relevant codes of conduct or other rules which are enforceable in that State or territory; and
- (h) any security measures taken in respect of the data in that State or territory.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Under the Data Protection Act 2020, the Eighth Data Protection Standard (see question 8.1) does not apply to a transfer where:

- (a) the data subject consents; or
- (b) transfer is necessary for the performance of/entering into a contract with the data subject;
- (c) transfer is necessary for the conclusion or performance of a contract between the data controller and a person other than the data subject which is:
 - (i) entered into at the request of the data subject, and
 - (ii) is in the interest of the data subject;
- (d) transfer is necessary for reasons of public interest;
- (e) transfer is necessary for legal proceedings, obtaining legal advice, or for establishing, exercising or defending legal rights;
- (f) transfer is necessary to protect the vital interests of the data subject;
- (g) the personal data to be transferred is included on a public register, and any conditions subject to which the register is open to inspection are complied with by any person to whom the data is or may be disclosed after the transfer; or
- (h) transfer is made on terms which are of a kind approved by the Commissioner as being made in such manner as to ensure adequate safeguards for the rights and freedoms of data subject.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Jamaica? Are there minimum standards? Does this differ by sector or size of the entity?

The Data Protection Act 2020 provides for data security regulation in Jamaica and outlines the standards for securing data to which companies must adhere.

Additionally, the Interceptions of Communications Act 2002 criminalizes the act of intentionally intercepting communication in the course of its transmission by means of a telecommunications network.

9.2 How are personal data breaches regulated in Jamaica? What are the requirements for notification and response?

Under the Data Protection Act 2020, a data controller must:

- (a) report to the Commissioner any contravention of the Data Protection Standards and any security breach which affects, or may affect, personal data within 72 hours after becoming aware of the contravention or security breach.

Such report must set out, inter alia:

- (i) the facts surrounding the contravention or security breach,
- (ii) a description of the nature of the contravention or security breach, including the categories, number of data subjects and type and number of personal data concerned, and
- (ii) the consequences of the breach and the measures taken or proposed to be taken to mitigate or address them; and
- (b) notify each data subject whose personal data is affected of:
 - (i) the nature of the contravention or breach,
 - (ii) the measures being taken or proposed to be taken in order to mitigate or address the possible adverse effects of the breach, and
 - (iii) the name and contact details of the data protection officer.

Where the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection standards, the Commissioner may serve the data controller with a notice with a view to achieving compliance.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

If a data controller does not comply with the standards for processing personal data, or fails to make a report to the Information Commissioner or notification to data subjects of a contravention of data protection standards or any security breaches (see question 6.2), the data controller may be liable (on summary conviction in the lower courts) to a fine of up to JMD 2 million (approx USD 12,500), or a prison sentence of up to 2 years, or, (on indictment in the upper court) to a fine set by the court or imprisonment for a term not exceeding 7 years.

A person who processes personal data without registering with the Commissioner is liable (upon summary conviction), to a fine of up to JMD 2 million or to imprisonment for a term not exceeding 6 months.

There are also remedies under the law of confidence for breach of confidence.

10.2 Do consumers have a private right of action? What remedies are available to them?

No. Individuals do not have a private right of action under the Data Protection Act 2020. However, individuals have a private right of action under constitutional law, torts and contract law. The potential remedies are damages.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

No enforcement action is currently being taken under the Data Protection Act 2020 by the OIC. At this stage, the OIC has been focused on compliance and particularly in registering data controllers that process large volumes of data or sensitive personal data. Likewise, the focus at this stage has been on raising public education and awareness. getting data controllers registered, rather than enforcement.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Jamaica?

The Data Protection Act 2020 is still in its early stages of implementation, and the current focus of the OIC has been on compliance and getting data controllers registered, rather than enforcement. The Act has represented a major cultural shift in the culture of doing business in Jamaica, as it restricts the processing and use of an individual's data, and data is often shared with other companies for the purposes of marketing.

In addition, in part because Jamaica's Data Protection Act 2020 was modelled on the European Union's GDPR, companies in Jamaica are being sensitized to the GDPR as well as the Data Protection Act 2020, and some companies that handle information of EU citizens are taking steps to implement its regulations.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Despite the Data Protection Act 2020 having come fully into effect, there are still challenges in encouraging compliance, including registering with the OIC under the Act. As previously mentioned, the OIC is currently solely focused on registering data controllers, and has not yet tackled the enforcement aspects of its powers. Companies will need to monitor how the role of the OIC evolves once registration has been completed and the focus shifts to compliance and enforcement rather than the administrative aspect of the Act.

Likewise, the Cyber Crimes Act 2015, which was reviewed in 2018, will have a major impact on companies.

There is also a National Identification Bill which has privacy implications. In its original format, this Bill was deemed unconstitutional in relation to the Constitutional right to privacy, but has subsequently been amended to remove the infringing sections.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

- (a) Although the Data Protection Act 2020 only covers 'personal data', the broader right to privacy is held in high regard by the local courts. Decisions from the courts in Jamaica have shown that the right to privacy is held highly as a constitutional right. Accordingly, companies should take care to protect an individual's privacy.
- (b) Companies in Jamaica are advised to meet the data protection standards, which have been implemented in the Data Protection Act 2020.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The Memorandum of Objects and Reasons for the Data Protection Act 2020 states that one reason behind the enactment of the Act was that Jamaica, as part of CARIFORUM, had entered into an economic partnership agreement with the European Union which requires signatory States to 'establish appropriate legal and regulatory regimes, in line with high international standards, with a view to ensuring an adequate level of protection of individuals with regard to the processing of personal data'.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The Data Protection Act 2020 will be transformative to Jamaica, as there will have to be major adjustments in current practices for companies to ensure compliance.

12.3 What do you envision the privacy landscape will look like in five years?

Within five years, it is anticipated that we will see enforcement actions being taken and an acknowledgement that these legal changes are not just theoretical but need to be implemented.

It is also anticipated that as public education and awareness grows, individuals will exercise their rights under laws such as the Data Protection Act 2020 and hold companies to a higher standard of accountability.

JAPAN

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Japan.

Privacy and the protection of personal information are rights arising under a mixture of constitutional, statute and case law.

1.2 What are the primary laws regulating privacy in Japan? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

An individual's (Japanese or foreign) right to privacy is protected under the Japanese Constitution and is construed as ranging from a right not to have one's private affairs intruded upon to the right to control one's own information. The right to privacy has also been recognized in tort law.

Privacy rights do not extend to corporations.

Other than the provisions of the Japanese Constitution, there are no laws specifically relating to the protection of privacy. Privacy rights (as opposed to the protection of personal information) are an undeveloped area of law in Japan when compared to those found in other developed nations, particularly in certain EU countries.

In addition, as regards personal information:

- (a) the Act on Protection of Personal Information ('APPI') and related guidelines govern the collection, storage, usage and processing of personal information in Japan.
- (b) Social security numbers (commonly known as 'My Numbers') are subject to a specific data protection regime under the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures, which is somewhat stricter than that under the APPI.
- (c) Guidelines relating to the APPI cover matters such as transfers of personal information to a third party in a foreign country, obligations on due diligence and recordkeeping when transferring personal information to a third party, and data anonymization.
- (d) Certain ministries have been delegated authority to issue guidelines for the implementation of the APPI for the industries they regulate ('Sector-Specific Guidelines'). There are Sector-Specific Guidelines in the finance, healthcare, telecommunication and postal sectors (issued by the Personal Information Protection Committee ('PPC') with the Financial Services Agency, the Ministry of Health, Labor and Welfare, the Ministry of Internal Affairs and Communications and the Ministry of Internal Affairs and Communication, respectively).
- (e) There are also supplementary rules on the handling of personal data transferred from the European Union and the United Kingdom on the basis of the EU adequacy decision concerning the APPI.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Japan Information Society Promotion Association established the Privacy Mark System and has operated it since 1998 in order to implement measures to protect personal information. The system evaluates businesses and other entities that comply with the Japanese Industrial Standards and properly protect personal information, and assigns a Privacy Mark to indicate compliance, which the recipient can use for business activities.

The purposes of the Privacy Mark are to raise consumer awareness of the protection of personal information and privacy through the use of visible privacy marks, and to provide business operators with an incentive to gain social trust in response to growing consumer awareness of the protection of personal information and privacy by promoting the appropriate handling of personal information private matters.

1.4 How is privacy law enforced in Japan? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The right to privacy and the APPI are enforced through the courts, bar associations, the PPC and other regulators in certain business sectors:

- (a) A person who believes their privacy rights have been infringed can apply to a court for injunctive relief and/or compensation for damages suffered.
- (b) The Japan Federation of Bar Associations ('JFBA'), in accordance with Article 1 of the Attorney Act ('The mission of lawyers is to protect fundamental human rights and to achieve social justice'):
 - (i) accepts requests for human rights relief from victims of human rights violations and related persons, including a person who has had their privacy violated,
 - (ii) investigates the facts of the requests and the facts of the violations, and
 - (iii) when it finds that human rights violations have occurred or are likely to occur, aims to eliminate or reduce them by taking measures such as issuing warnings, recommendation or requests (in each case, providing its opinions and seeking/urging appropriate responses), to those who have or may commit the violations and/or their supervisory authorities, if any.

In order to ensure that the measures proposed are implemented, the JFBA makes inquiries of the parties after a certain period of time regarding cases in which warnings, recommendations, requests, and other measures were taken. If the answer is not sufficient, a second inquiry may be made (post action inquiry). Although the above human rights remedies are not legally enforceable, they are influential in practice, and in many cases they are complied with, and this procedure has gained the public's trust.

- (c) The PPC is the primary regulatory body for data protection in Japan, and is responsible for supervising entities handling personal information which are subject to the APPI and for regulation of the handling of My Numbers. If Sector-Specific Guidelines have been issued, the issuing regulator will be responsible for enforcing them.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Japan?

All companies are subject to Japan's privacy laws. The APPI applies to a business operator using a personal information database for its business—a 'personal information controller' ('PIC')—and the handling of that information by the PIC, but does not apply to:

- (a) broadcasting institutions, newspaper publishers, communication agencies and other press (including individuals engaged in news reporting as their business) for the purpose of news reporting, which means informing many and unspecified individuals or entities of objective facts as fact (as well as opinions or views based on such facts);

- (b) a business operator that conducts literary work as its business, for the purpose of literary work;
- (c) religious organizations for the purpose of religious activities (including incidental activities); and
- (d) political organizations for the purpose of political activities (including incidental activities).

However, such entities must endeavor to take the necessary and appropriate measures to control the security of personal information, to ensure the proper handling of personal information, and for the processing of complaints about the handling of personal information, and must also endeavor to announce publicly the content of those measures.

‘Handling’ is regarded as collection (acquisition), retention, use, transfer and any other acts of handling personal information.

2.2 Does privacy law in Japan apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The constitutional right to privacy does not apply to companies outside Japan. Certain obligations under the APPI apply to a company outside Japan where it handles personal information as part of a business and, in relation to supplying a good or service to a person in Japan, has acquired personal information relating to the person or has anonymously processed information produced by using that personal information. The obligations which apply extra-territorially include:

- (a) to specify and notify or publicize the purpose of utilization of the personal information, and to use it within that purpose;
- (b) to keep personal data (ie, personal information held on a database) accurate and up-to-date, and to delete it when no longer required;
- (c) to take measures to protect the personal data against leaks, etc;
- (d) to supervise employees handling personal data and any service provider entrusted with the handling of personal data;
- (e) to comply with the rules governing disclosure to a third party;
- (f) to publicize privacy policies;
- (g) to comply with the rights of a data subject to access, correct, and stop the illegal use of their personal data; and
- (h) to comply with certain rules regarding anonymized information.

There is no requirement that such a company have a representative in Japan.

The PPC may also request reports from, and issue orders to, an offshore PIC (ie, a foreign business operator), and may disclose the name of the business operator in the event of non-compliance with such orders. In addition, the PPC may provide information to foreign regulatory authorities for their own regulatory enforcement purposes.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Japan?

‘Personal information’ is defined under the APPI as information relating to a living individual in Japan which falls under any of the following items:

- (a) information containing a name, date of birth, or other descriptions, etc (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed

using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form ie, an electronic, magnetic or other form that cannot be recognized through the human senses) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual); and

- (b) information containing an individual identification code. An 'individual identification code' includes:
 - (i) characters, numbers, symbols and/or other codes for computer use which represent certain specified physical characteristics (such as DNA sequences, facial appearance, iris patterns, vocalizations, posture and walking movements, finger and palm prints, and vein patterns) and which are sufficient to identify a specific individual,
 - (ii) certain identifier numbers, such as those on passports, driver's licenses and resident's cards, and the 'My Number' individual social security number,
 - (iii) unique characters, numbers, symbols and other codes designated by the enforcement ordinance of the APPI that are assigned to and specified on health and care insurance cards, and
 - (iv) any characters, numbers, symbols and other codes designated by the Enforcement Rules of the Personal Information Protection Commission as being equivalent to any of the above.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

'Sensitive personal information' means any personal information relating to matters such as physical or mental disabilities, medical records, medical and pharmacological treatment, and arrest, detention or criminal proceedings (whether as an adult or a juvenile). It is necessary to obtain consent from the data subject in order to obtain or transfer sensitive personal information unless one of the exceptions discussed at question 8.1(a) applies. The opt-out system (deemed consent given where the data subject has been given the chance to refuse consent but has not done so) cannot be used for a transfer of sensitive personal information.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

- (a) **Anonymized information** refers to information relating to an individual that has been processed from personal information by deleting parts of the descriptions such as name and date of birth, and removing all personal identification codes, so that a specific individual cannot be identified. It must also be processed in a way that ensures the original personal information cannot be restored and the individual cannot be re-identified.

A PIC that creates anonymized information must process the data appropriately during its creation. Once anonymized information is created, the operator must implement security control measures regarding the processing methods and publicly disclose the types of information contained in the anonymized dataset.

When anonymized information is provided to a third party, the categories of information and method of provision must be publicly disclosed, and the recipient must be explicitly informed that the information is anonymized.

When using anonymized information, the business handling it must not attempt to identify the individual to whom the original personal information relates by cross-referencing it with other information.

- (b) **Pseudonymized information** refers to information relating to an individual that has been processed from personal information in such a manner that specific individuals cannot be identified unless it is collated with other information. This includes the partial deletion of entries such as name or date of birth, and the complete removal of personal identification codes.

A business handling pseudonymized information must not process it beyond the scope necessary to achieve the specified purpose of use, except where permitted by law. Unless the purpose of use has been previously disclosed, it must promptly be made public.

Except as required by law, pseudonymized personal data must not be provided to third parties. Furthermore, similar to ordinary personal information, the handling of pseudonymized information is subject to rules including: prohibition of improper use, proper acquisition, implementation of security control measures, supervision of employees and contractors, and procedures for handling complaints.

Although pseudonymized information may, in some cases, not fall under the definition of personal information, it must not be provided to third parties except where permitted by law. Provisions regarding security control measures, supervision of employees, supervision of contractors, handling of complaints, prohibition of re-identification, and prohibition of contacting the data subject are applicable to such information.

- (c) There is no definition of de-identified data in Japan.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

A PIC must:

- (a) not collect personal information by fraudulent or other unlawful means;
- (b) before acquiring personal information, notify the data subject of the purpose of use of the personal information or publish that purpose of use in a manner accessible to the data subject;
- (c) only obtain, use, maintain and transfer personal information within the scope of the purpose of use;
- (d) implement safety management measures for the acquisition, storage and use of personal information, and the appropriate supervision of employees and contractors; and
- (e) notify each data subject of the procedure for the data subject to require correction, etc, of their personal data and where to complain about the PIC's handling of personal data.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No, there are no specific roles based on how personal information is held or processed in Japan; a data holder/controller is the PIC under the APPI (see the description above), and although 'processor' is not defined by the APPI, it is broadly regarded as an entity to which a PIC entrusts the handling of personal data in whole or in part within the scope necessary for the achievement of the purpose of

utilization (eg, entrusting personal data to a service provider such as a cloud computing service provider or a mailing service provider for the purpose of having them provide the PIC with the services). A data processor which is not a PIC is not regulated under the APPI, though the PIC which instructs it will have supervision and similar obligations.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

No.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

It is necessary to specifically identify the use of the collected personal information for advertising purposes and include that information in the privacy notice.

As example, it is necessary to clearly specify how the personal information will be used, such as:

- (a) analyzing collected browsing and purchase history data to deliver advertisements for new products and services tailored to the user's interests and preferences; or
- (b) analyzing collected purchase history data to calculate a credit score, and providing that score to third parties.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) If requested by a data subject, a PIC must disclose, without delay, to the data subject the data subject's personal data held by it, in the method requested by the data subject (eg, as electronic data) unless the required method is financially unreasonable (in which case, in writing). Access can be refused if it would result in:
 - (i) injury to the life or bodily safety, property or other rights and interest of the data subject or any third party;
 - (ii) a material interference with the PIC's business operations; or
 - (iii) a violation of other Japanese laws prohibiting disclosure.
- (b) Data subjects also have the right to revise, correct, amend or delete their personal data, and to request cessation of use of their personal data:
 - (i) if this is used for a purpose other than the one originally stated;
 - (ii) if it was acquired by fraudulent or other unlawful means;
 - (iii) if there is no longer a need to use the data;
 - (iv) when a data breach has occurred; or
 - (v) if there is a likelihood of infringement of the data subject's rights or lawful interests due to the PIC's handling of the personal data.

If a data subject requests a PIC to cease using their personal data, the PIC must do so unless the request is unreasonable, or the cessation would be costly or would otherwise be difficult (eg, the recall of books already distributed).

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies must obtain consent from data subject and/or provide opt-out options to use personal information for advertising activities. It is necessary to notify the data subject in advance, or to place the relevant information regarding 'opt-out' in a manner readily accessible to the data subject and report the 'opt-out' to the PPC.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

A PIC is required to supervise its contractors, such as advertising agencies, DSPs, SSPs, or data providers to ensure that they manage personal information appropriately. There is no difference in the extent of obligations depending on the type of vendors.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

A PIC is required to record any provision of personal information to third parties under the APPI. When a PIC receives personal information, it is required to confirm the information about the provider and the circumstances surrounding the acquisition of the personal information. However, there are no specific contractual obligations.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

It is expected that companies will constantly check that personal information is being handled appropriately.

Under the Privacy Mark System, which is utilized by many advertising companies, businesses must conduct internal audits at least once a year and as necessary to confirm whether their personal information protection management system meets the following criteria, that:

- (a) the company's internal regulations (including requirements established by the company itself) comply with the requirements of this guideline; and
- (b) the personal information protection management system is effectively implemented and maintained.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Under the APPI, personal information (such as name, address, email address and telephone number) may not be used outside the scope of the specified purpose of use without the consent of the data subject. If a marketer (as a PIC) breaches these requirements (eg, using the email address of a data subject which was not provided by the data subject or published), it will infringe the personal information of the data subject, especially for B2C marketing.

Explicit consent is usually required for sending marketing communications. No entity or individual is permitted to send an email and/or text message containing commercial advertising without the recipient's explicit consent or prior request under the Act on Regulation of Transmission of Specified Electronic Mail.

Marketing emails, messages, etc, must contain prescribed information. This includes expressly indicating the true identity and contact details of the sender in such marketing emails, etc, and contact details (URL or email address) to opt out of receiving further marketing emails, etc.

If the email, etc, is related to mail order sales, it is prohibited, under the Act on Specified Commercial Transactions, for a seller or a service provider to advertise via email, etc without the consent of the advertising target, except:

- (a) when sending email, etc, advertising regarding the terms and conditions under which the seller or the service provider sells goods or specified rights or provides services through mail order sales ('mail order email') at the request of the advertising target;
- (b) when sending an email, etc, with important matters related to the mail order email, such as confirmation of an agreement, order confirmation, delivery notification, with advertising as a part of the email; or
- (c) when sending an email, etc, that advertises mail order sales where the competent ministry has found such to be unlikely to prejudice the interests of the target of the email.

Even if a seller or service provider has obtained an advertising target's consent or request to send a mail order email they may not do so if the target later indicates an unwillingness to receive the email.

When sending a mail order email, a seller or service provider must keep a specified record of the consent of the advertising target or of having received a request from the advertising target to send the email, and must preserve those records.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Cookies and website browsing/web form entry history data associated with the cookies (together referred to as 'cookies etc') are not personal information unless the relevant data subject can be identified by easy reference to, or combination with, other information in Japan (eg, when a company's online 'signed-up' customers in Japan log in to the company's website and then browse, search flights, etc, where the cookies of their browsing and flight search history are tied to the specific individuals who logged in online, the data are thus person-identifiable). Generally, cookies etc are not considered personal information, so consent of the data subject is not required for their transfer. However, even if cookies etc are not personal information for a transferor in this sense, the transfer will be a transfer of person-related information, and thus subject to the consent requirements referred to above, if the cookies etc are transferred to a third party transferee and would be personal information for the transferee, as the transferee holds other information, and the individual related to the cookies etc can be identified by reference to such other information. An example of this would be where the cookies etc are a history of website browsing that suggests an individual's activity behavior, preference of goods/services, or is otherwise usable for profiling, and the transferee would use the cookies etc for targeted advertising, or for an assessment of the individual's application for a job position or for financial services, etc). As to person-related information please see question 12.3.

7.3 How are loyalty programs and promotions regulated under privacy law?

There is no specific regulation on loyalty programs and promotions from a privacy or data protection perspective although the APPI applies to loyalty programs and promotions.

7.4 How is social media and influencer marketing regulated under privacy law?

There is no specific regulation on social media and influencer marketing from a privacy or data protection perspective.

The Japanese government has raised concerns about privacy on social media, and the Ministry of Internal Affairs and Communications has raised awareness by posting ‘precautions when using social networks’ on its website ‘the information security website for citizens’.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are no specific regulations on targeted advertising and behavioral advertising.

However, the Japan Interactive Advertising Association, formed by companies involved in the internet advertising business such as media and advertising companies, has produced Guidelines on Targeting Advertising. These Guidelines stipulate that advertisers should be aware that behavioral history information may involve users’ privacy and should conduct behaviorally targeted advertising with consideration for the users.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution often involves handling personally identifiable information (‘PII’) which may require the consent of data subject and adherence to data protection regulations under the APPI. There are no specific regulations on clean room technologies under privacy law. To avoid treating the data transfer as a provision to a third party—which would require the data subject’s consent—it is common to structure the use of clean room technologies as a form of joint use among the parties involved.

7.7 How is location-based advertising regulated under privacy law?

There are no specific regulations on location-based advertising.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific privacy rules governing data brokers; but, if the data broker is a PIC, the data handling, transfer, etc, obligations under the APPI would apply to it and the PIC should record the transfer of personal data to a third party in accordance with the APPI Guidelines (see question 9.1 below).

7.9 How is advertising to children and minors regulated under privacy law?

Under privacy laws, there are no specific regulations concerning children or minors from an advertising perspective. However, since the capacity to consent to the handling of personal information is generally recognized from around ages 12 to 15, depending on the nature of the content, it is considered necessary to obtain the legal guardian’s consent for children below that age range. Accordingly, in practice, parental consent is typically sought when collecting personal information from minors in promotions or similar activities targeting them.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific regulations concerning profiling of the use of artificial intelligence or automated decision-making technology for advertising purposes.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

- (a) **General Rules:** A PIC which holds personal information must not transfer personal data (ie, personal information compiled in a personal information database, etc) to a third party without obtaining the data subject's consent to do so in advance, except if:
- (i) the PIC provides the third party with personal data as permitted by laws and regulations;
 - (ii) it is necessary for the PIC to provide the third party with the personal data in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the data subject;
 - (iii) there is a special need for the PIC to provide the third party with the personal data in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the data subject;
 - (iv) it is necessary for the PIC to provide the third party with the personal data in order to cooperate with a national government organ, local government, or an individual or a business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the data subject is likely to interfere with the performance of those affairs; or
 - (v) the transfer is made pursuant to an 'opt out' which satisfies conditions specified by law and guidelines (see question 8.2) (Note that this exception does not apply to sensitive personal information).

Anonymized information may be transferred to a third party without the consent of the original data subject (as it will no longer constitute personal information), provided that the transferor PIC makes public both the fact of the transfer and what types of personal information are included in it, and notifies the recipient that the information is anonymized information.

- (b) **Transfer to third party:** Guidelines clarify that the exchange/transfer of personal data between subsidiaries, jointly controlled companies and group companies; between a franchisor and its franchisees; or between the same professions/industry is considered to be a transfer to a third party unless deemed otherwise.

However, a person being provided with personal data is not deemed to be a third party for the purpose of the transfer of data:

- (i) if it is a person to whom the PIC has entrusted all or part of the handling of the personal data within the scope necessary for achieving the purpose of use;

- (ii) if the personal data is provided to the person when it succeeds to the business of the original PIC due to a merger or similar circumstances; or
- (iii) if personal data is used jointly by PICs, provided that they either notify the person (data subject) in advance of:
 - this joint use,
 - the items of the personal data used jointly,
 - the extent of the joint users,
 - the purposes of joint use, and
 - the name of the individual or business operator who is responsible for managing the personal data,
 or make the foregoing information readily accessible to the person in advance.
- (c) **Transfers Offshore:** The transfer by a PIC of personal data to a third party in a foreign country (other than in reliance on one of the exceptions listed in (a) above) is subject to the following requirements in addition to those generally applicable to transfers of personal data:
 - (i) where consent to the transfer is given by the data subject, it must be clear that it covers the transfer to a third party in a foreign country; and the data subject must be provided, when giving the consent, with information necessary for judging whether to provide the consent (eg, the foreign country is identified or identifiable or the circumstances where such data transfer will be made have been clarified); or
 - (ii) in the absence of such consent, if the transferor wishes to rely on an opt-out or the fact that the transfer is not to a third party as an exception to the requirement to obtain the data subject's consent to the transfer, it is also necessary that the transferee:
 - is in a country on a list of countries issued by the PPC as having a data protection regime equivalent to that under the APPI (Only countries in the European Union, the United Kingdom and the European Economic Area are on the list of countries); or, if the country of the transferee is not on the list of countries,
 - implements data protection standards equivalent to those which PICs subject to the APPI must follow. Such an equivalent standard can be satisfied:
 - by the transferor and the transferee entering into a contract; or
 - (if the transferor and the transferee are in the same corporate group) by both being subject to binding standards of the group for the handling of personal data, pursuant to which the transferee is subject to all the obligations imposed by the APPI on PICs who are subject to it, and which must include certain specified matters, such as purpose of use, record-keeping and details of security measures; or
 - where the transferee is accredited under APEC's Cross Border Privacy Rules system (a system for building trust among consumers, businesses and government agencies for personal information distributed across borders in the APEC region).

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

- (a) **Record keeping:** A transfer of personal data requires that the transferor PIC and the transferee (if a PIC, or if it becomes a PIC as a result of the transfer) keep specified records, and the transferee is also required to make enquiries as to the source of the personal data transferred. Both records and enquiries are required unless the transfer was made in reliance on an exception (see question 8.1(a)) or the transferee is not a third party.

Thus:

- (i) the transferor must keep a record of:
 - (if the transfer was made in reliance on an opt-out) the transfer date;
 - the name or other identifier of the transferee and the data subject, and the type(s) of data transferred (eg, name, age, gender); and
 - the data subject's consent to the transfer, or, if consent has not been obtained and the transfer was made in reliance on the opt-out, that fact.
- (ii) The transferee must keep a record of:
 - (if the transfer was made in reliance on an opt-out) the date it received the personal data;
 - the name or other identifier of the transferor and its address (and the name of its representative if the transferor is a legal entity), and the name of the data subject;
 - the type(s) of data transferred;
 - the data subject's consent to the transfer, or, if the consent has not been obtained and if the transfer was made in reliance on an opt-out, that fact;
 - if an opt-out has been relied on, the fact that the opt-out has been filed with, and published by, the PPC; and
 - how the transferor acquired the personal information transferred (having first ascertained this).

- (b) **Opt-outs:** Personal data (other than sensitive information) can be transferred using an opt out (ie, a system whereby a data subject is notified of the proposed transfer of its personal information to a third party and given the opportunity to object to that transfer) to obtain consent, but only after the PIC has notified the data subject of, or made readily available to the data subject, and filed with the PPC, all of the following information, and a period necessary for the data subject to exercise its opt-out right has expired:

- (i) that the transfer is within the scope of the originally stated purpose of utilization;
- (ii) the specific personal data to be transferred;
- (iii) the means with which the personal data will be transferred;
- (iv) the fact that the transfer of the personal data is subject to an opt-out; and
- (v) where to provide such opt-out exercise notice.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Japan? Are there minimum standards? Does this differ by sector or size of the entity?

The APPI requires a PIC to take necessary and appropriate action for the security and control of personal data held by it, including preventing the leak, loss or damage of the personal data.

APPI Guidelines require the following measures for data security:

- (a) preparation of basic policies;
- (b) establishment of discipline on the handling of personal data;
- (c) organizational safety management measures (ie, establishment of an organizational system, operation in accordance with regulations on the handling of personal data, establishment of means to confirm, and establishment of a system for responding to leaks);
- (d) personnel management measures (employee education);
- (e) physical safety management measures (ie, management of areas where personal data is handled, prevention of leaks, deletion of personal information, disposal of electronic media); and
- (f) technical safety control measures (access control, preventing unauthorized access).

There is no minimum standard required by the APPI Guidelines, though they do provide examples for data security standards.

9.2 How are personal data breaches regulated in Japan? What are the requirements for notification and response?

The APPI and the regulations of the PPC set forth measures with regard to data breaches, for which detailed explanations are provided in the PPC's guidelines, as follows:

- (a) It is desirable to take the following actions following a data breach:
 - (i) internal reporting and prevention of expansion or aggravation of any damage;
 - (ii) investigation of the facts and investigation of the cause;
 - (iii) identification of the scope of the impact of the breach;
 - (iv) review and implementation of measures to prevent a recurrence;
 - (v) prompt contact with the affected person(s) unless the leaked data is encrypted at a high level; and
 - (vi) publication of facts and measures to prevent a recurrence.
- (b) The PIC must promptly (within 3 to 5 days) notify the PPC of a breach if:
 - (i) the affected (or possibly affected) data contains sensitive information;
 - (ii) the affected (or possibly affected) data would cause a financial risk in the case of unauthorized use;
 - (iii) the loss is as a result of intentional theft or possible theft by a third party (as opposed to just an accidental loss); or
 - (iv) the number of affected (or possibly affected) data subjects exceeds 1,000.
- (c) The PIC must also make efforts to promptly notify the PPC of a breach unless:
 - (i) the leaked data is encrypted at a high level;
 - (ii) all the leaked data has been collected by the PIC prior to being seen by third parties;
 - (iii) there is no risk of any specific individual being identified from, or the affected data subjects being harmed by use of, the leaked data;
 - (iv) the data loss was obviously only internal and not an external leak; or
 - (v) the leak is obviously insignificant (eg, a mis-delivery of parcel where the personal information is only on the delivery address label).

In practice, a PIC suffering a data breach should always consider consulting local counsel to assess the severity of the breach and the advisability of reporting to the PPC, and if and how to notify affected data subjects.

Where a PIC has entrusted personal data to a personal information/data processor and the personal information/data processor was subject to the data loss, the obligations above fall on the PIC, though those obligations may be satisfied to the extent the personal information/data processor makes the required report.

The PPC has published a reporting form on its website (only available in Japanese).

If a data loss has occurred and been reported to the PPC, mandatorily, voluntarily or at the request of the PPC, the PPC may investigate the background to the loss, the PIC's data management procedures, and the actions the PIC has taken (or not taken) to notify the affected parties (and the PPC). The PPC may then issue guidance on what actions the PIC should take.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The APPI provides criminal penalties for violation of personal data security. For example, a PIC (or its director, representative or administrator if it is a corporate body), its employee, or a person who used to be such a business operator or employee, which has provided, or used by stealth, personal information databases etc, (including wholly or partially duplicated or processed ones) that they handled in relation to their business for the purpose of seeking their own or a third party's illegal profits, may be punished by imprisonment with work for not more than one year or a fine of not more than JPY 500,000 (approx USD 3,500).

If the PPC has issued an order for improvement in respect of a data breach, failure to comply with it will render an individual who is the PIC, or the director or employee of the PIC in charge of the breach if the PIC is an entity, liable to possible criminal imprisonment for up to one year or a criminal fine of up to JPY 1,000,000 (approx USD 7,000), and the same criminal fine for the PIC as an entity.

In addition, if a representative of a corporation, or an agent, employee, or other worker of a corporation or an individual, violates an order of the PPC in connection with the business of that corporation or individual, or provides personal information to a third party for fraudulent purposes, in addition to punishing the individual responsible for the act, the corporation may also be subject to a fine of up to JPY 100 million (approx USD 70,000).

Further, many Sector-Specific Guidelines authorize the relevant regulators to enforce the APPI and guidelines by rendering business improvement orders, or business suspension orders in the worst cases, against providers of services, which require licenses from the regulator 'where necessary for ensuring the appropriate operation of the business'.

10.2 Do consumers have a private right of action? What remedies are available to them?

Data subjects may seek compensation for breaches of the APPI which relate to their personal information and which cause them loss. The compensation paid in such cases has ranged from JPY1,000 per data subject in a broad leakage case to several million yen for a violation of privacy. PICs which have suffered a data loss have often voluntarily offered compensation to affected parties, both to forestall any proceedings, and to maintain good public relations.

Actions for breach of the constitutional right to privacy or breach of privacy in tort can be brought before the courts, though such actions are rare.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The PPC primarily receives reports of personal data breach incidents and is mainly responsible for monitoring, supervision, guidance, and providing advice on PICs. It generally does not take an active role in direct intervention. The PPC is not expected to initiate litigation on its own. However, there has been a case in which the PPC filed a criminal complaint against a business operator that failed to report, or submitted a false report, in response to the PPC's request following an incident involving the unauthorized removal of personal information.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Japan?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

The obligation to report data breaches to the PPC under the APPI is stricter when compared to legal frameworks in other countries. For example, in the case of a cyberattack on a global company leading to a personal data breach, some countries' laws adopt a risk-based approach, potentially exempting the company from reporting to authorities. However, in Japan, any loss or leakage of personal data requires reporting to the PPC, regardless of the severity, unless an exception (eg, the data in question is encrypted at a high-level) applies (see question 6.2). Businesses should be mindful of this strict regulatory requirement.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The key change since 2022 is the full enforcement of the 2021 Amendment to the APPI. The 2021 Amendment was intended to adapt to the evolution of the digital society and unify the personal information protection framework between national and local entities, ensuring more effective personal data management and protection. Key features include:

- (i) **Unification of national and local personal information protection systems:** The amendment standardized the rules across the country, ensuring that personal information is managed under a unified legal framework rather than individual municipal ordinances.
- (ii) **Adaptation to the Digital Society:** With advancements in digital technology, the use of online services and AI-based technologies has increased, bringing new risks to personal data security. The 2021 Amendment addressed these emerging risks. For instance, stricter regulations on anonymized processed information and clearer rules on cross-border data transfers were introduced.

- (iii) **Strengthening the authority of the PPC:** Previously, local governments managed their own personal information protection policies, but under the amendment, the PPC now has centralized oversight. This ensures stricter management of personal information protection and faster responses to violations.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

- (a) Broader regulation and intervention by the PPC, in particular, in cross-border data transfers and data leaks.
- (b) As regulations will be tightened to protect personal information and privacy, it will be necessary to establish internal regulations to enable compliance with regulations, and to ensure that employees fully understand the importance of privacy.
- (c) Cyber-attacks are becoming more sophisticated; in order to avoid the risk of data leaks, it is necessary to review data security in a timely manner and ensure the security level of the equipment used.
- (d) As global harmonization of regulations and the extraterritorial application of national information protection laws is expected to be widespread, it is necessary to collect information on, and update, not only national laws, but also relevant national information protection laws, and to respond as necessary.

12.3 What do you envision the privacy landscape will look like in five years?

- (a) The PPC follows a principle of ‘reviewing every three years’ which is prescribed in the 2021 Amendment of the APPI. Since November 2023, it has been conducting a detailed examination through fact-finding efforts on international trends in personal information protection, advancements in information and communication technology, the creation and development of new industries utilizing personal data, and the enforcement status of existing laws. This process also involves hearings from various stakeholders. In July 2024, the PPC released an interim report on the review. The main points under consideration include:
 - (i) **More substantive protection of individuals’ rights and interests:** Addressing issues such as the handling of biometric data, improper use and acquisition of personal information, opt-out mechanisms, the treatment of children’s personal data, and claims for injunctions and damage recovery by organizations;
 - (ii) **Effective monitoring and supervision:** Exploring measures such as administrative oversight tools (surcharges, recommendations, and orders), criminal penalties, and reporting and notification requirements for data breaches; and
 - (iii) **Support for initiatives to promote data utilization:** Considering frameworks for utilizing data without requiring individual consent.
- (b) Regarding person-related information, such as a phone number, email address, or cookie ID, if a business possesses data that enables direct contact with an individual, there is a recognized risk that handling such information could infringe on privacy and other individual rights and interests. Depending on how the business uses this information, the extent and likelihood of such infringement could be as severe as with personal information. Therefore, it has been highlighted that appropriate measures must be considered to prevent improper acquisition and misuse.

- (c) Under the current APPI and other laws, there are no explicit provisions regarding the handling of children's personal information. The only regulations in place pertain to disclosure requests made by legal guardians and the requirement for a guardian's consent in place of the child's own consent. At the international level, organizations such as the United Nations Committee on the Rights of the Child and the OECD have issued documents emphasizing the need for protective measures, considering children's immaturity and vulnerability. In light of these international frameworks, discussions are underway on how to address the required protections for children's privacy.

 KENYA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Kenya.

Currently, privacy in Kenya is regulated by a layered legal framework which sets out the legal obligations, rights and remedies that apply to public and private entities as well as individuals that process personal data. The fundamental right to privacy is primarily enshrined in the provisions of the Constitution of Kenya 2010 and in the provisions of the Data Protection Act 2019 ('DPA') and the Data Protection Regulations thereunder, as well as various other statutes, regulations, guidelines and court judgments. The DPA, which came into effect on November 25, 2019, is intended to give effect to the right to privacy as provided for in the Constitution. The DPA and the accompanying Data Protection Regulations set out the rights of data subjects and duties of data controllers and data processors, as well as the data protection principles that apply to the processing of personal data. These principles are binding on data controllers and data processors, whether public or private entities, that process personal data of data subjects who are located in Kenya.

1.2 What are the primary laws regulating privacy in Kenya? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The general framework of statutes that regulate privacy in Kenya includes:

- (a) Constitution of Kenya 2010 ('Constitution');
- (b) DPA;
- (c) Data Protection (General) Regulations 2021 ('General Regulations');
- (d) Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021 ('Complaints Regulations');
- (e) Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 ('Registration Regulations');
- (f) Access to Information Act 2016; and
- (g) Computer Misuse and Cybercrimes Act 2018 ('Computer Misuse Act').

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays a significant role in privacy regulation by allowing companies to establish and enforce their own data protection standards. In this regard, industry groups and organizations often develop codes of conduct, best practices, and compliance frameworks to ensure responsible data collection, use, and sharing to prevent the immediate need for strict government oversight.

Self-regulation in privacy and advertising in Kenya takes into account the provisions of the legal framework established by the DPA and its Regulations. This means that while companies may develop and comply with internal privacy policies and industry-led standards, they must still align with the statutory obligations under the DPA. Ultimately, while self-regulation in Kenya's advertising industry enables flexibility and innovation, it must operate within the strict legal boundaries set by the evolving regulatory framework. If industry-led initiatives fail to ensure adequate protection for the rights of data subjects, the Office of the Data Protection Commissioner ('ODPC') is likely to impose stricter enforcement measures to uphold data privacy standards.

1.4 How is privacy law enforced in Kenya? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Both the Courts and sector-specific regulatory bodies such as the ODPC and the Communication Authority of Kenya enforce provisions of privacy law in Kenya. The DPA provides for the establishment of the ODPC, whose functions include overseeing the implementation and enforcement of the DPA, the establishment and maintenance of the register of data controllers and data processors (set out under the Registration Regulations) and investigating any complaints relating to any purported infringement of any of the provisions of the DPA (set out under the Complaints Regulations).

The Complaints Regulations provide for the issue of enforcement notices and penalty notices, the procedure for hearing and determining of complaints and the resolution of complaints by means of alternative dispute resolution.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Kenya?

- (a) The Constitution is binding on all State organs and all persons. It provides that all persons have the right to privacy. The Constitution defines a ‘person’ to include a company, association or other body of persons, whether incorporated or unincorporated. As such, any company operating, or otherwise providing services, in Kenya is bound by the Constitution, whether or not such companies are incorporated in Kenya.
- (b) The DPA applies to all data controllers and data processors who:
 - (i) are established or ordinarily resident in Kenya and process data while in Kenya, or
 - (ii) are not established or ordinarily resident in Kenya but who process the personal data of data subjects in Kenya (whether or not the data subject is a Kenyan citizen).
- (c) The Access to Information Act applies to both public and private bodies. Its main objects include to:
 - (i) give effect to the Constitutional right to access information;
 - (ii) provide a framework for public entities and private bodies to proactively disclose information that they hold and to provide information on request in line with the constitutional principles; and
 - (iii) provide a framework to facilitate access to information held by private bodies in compliance with any right protected by the Constitution and any other law.

2.2 Does privacy law in Kenya apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. The DPA applies to companies registered or otherwise located outside of Kenya that process personal data of data subjects located in Kenya. Such foreign companies would be required to comply with the obligations under the DPA and the Regulations enacted thereunder.

The Registration Regulations, for instance, prescribe the requirements for mandatory registration by data controllers and data processors with the ODPC. This registration requirement applies whether or not the company concerned has an establishment in Kenya.

As regards the requirement for a local representative, the DPA provides that a data controller or data processor ‘may’ appoint a data protection officer where the core activities of the data controller or processor require the regular and systematic monitoring of data subjects or where the core activities entail processing sensitive categories of personal data. However, this is not a mandatory requirement.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Kenya?

Under the DPA, ‘personal data’ is any information relating to an identified or identifiable natural person. An ‘identifiable natural person’ means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the person’s physical, physiological, genetic, mental, economic, cultural or social identity.

Under the Access to Information Act, ‘personal information’ is somewhat broader and is defined to include:

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, age, physical, psychological or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
- (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- (c) any identifying number, symbol or other particular assigned to the individual;
- (d) the fingerprints, blood type, address, telephone or other contact details of the individual;
- (e) correspondence sent by the individual that is of a private or confidential nature, or further correspondence that would reveal the contents of the originating person’s opinion or views over another person;
- (f) any information given in support of or in relation to an award or grant proposed to be given to another person; or
- (g) contact details of an individual.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The DPA defines ‘sensitive personal data’ as data revealing a natural person’s race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details (including names of the person’s children, parents, spouse or spouses), sex or the sexual orientation of the data subject. ‘Biometric data’ is data resulting from specific technical processing based on physical, physiological or behavioral characterization, including blood typing, fingerprinting, DNA analysis, earlobe geometry, retinal scanning and voice recognition. The ODPC may prescribe further categories of personal data which may be classified as sensitive personal data at any time.

Under the DPA, sensitive personal data must be processed in accordance with the overriding data protection principles set out in the DPA. These principles, referred to as the ‘Data Protection Principles’, require every data controller and processor to ensure that personal data is:

- (a) processed in accordance with the right to privacy of the data subject;
- (b) processed in a lawful, fair and transparent manner;
- (c) collected for an explicit, specified and legitimate purpose;

- (d) adequate, relevant and limited to what is necessary;
- (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- (f) accurate and kept up-to-date;
- (g) kept in a form which identifies the data subject and for no longer than is necessary; and
- (h) not transferred outside of Kenya unless there is proof of adequate data protection safeguards, or the consent of the data subject is obtained.

Where sensitive personal data is processed outside of Kenya, the consent of the data subject must be obtained prior to any such processing activities (including cross-border transfer) and there must be a confirmation of appropriate safeguards being in place.

Furthermore, sensitive personal data which relates to the health of a data subject may only be processed by or under the responsibility of a healthcare provider or by a person subject to the obligation of professional confidentiality under any law. Moreover, the Health Act imposes additional confidentiality obligations regarding health data. It provides that information concerning a user, including information about their health status, treatment or stay in a health facility, is confidential except where such information is disclosed under a court order or informed consent or for health research and policy planning purposes.

3.3 **How are anonymized, pseudonymized, or de-identified data treated under privacy law?**

The DPA provides for the anonymization or de-identification of personal data to ensure that the data subject can no longer be identified. It requires the anonymization of a data subject's data where possible when using personal data for commercial purposes. A data controller or processor is considered to be using personal data commercially when, *inter alia*, it promotes products, services, or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services using consumer data. Moreover, data should also be anonymized or pseudonymized at the expiry of the data retention period or the lapse of the purpose for which the personal data was collected. Where personal data is anonymized in a way that it would not be possible to re-identify a data subject, the obligations under the DPA would not apply to such personal data.

4 **COMPANY OBLIGATIONS**

4.1 **What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?**

- (a) The DPA and the framework of various statutes that uphold the right to privacy maintain that, when dealing with personal information, data subjects must be made aware of their rights under the DPA. The rights are:
 - (i) to know how the information will be used;
 - (ii) to access the data;
 - (iii) to object to the processing of their data;
 - (iv) to request the correction of false or misleading data; and
 - (v) to request the erasure of false or misleading data.

These rights must be observed and upheld in addition to the Data Protection Principles highlighted in question 3.2.

- (b) There must be a lawful basis for the processing of personal data (usually consent), and a data controller or data processor may not process personal data without the consent of the data subject except where the processing is necessary for certain prescribed circumstances (see question 4.3).
- (c) Consent may be withdrawn at any time.
- (d) With regard to data minimization, data controllers and processors are required to ensure that the personal data processed is adequate, relevant and limited to what is necessary.
- (e) To ensure compliance with the transparency requirement, the General Regulations require data controllers and processors to develop, publish and regularly update a policy reflecting their personal data handling practices. The policy should include, *inter alia*:
 - (i) an outline of the categories of personal data collected,
 - (ii) data subject rights,
 - (iii) the lawful basis being relied upon,
 - (iv) whether or not personal data is being transferred outside of Kenya, and
 - (v) information on the controller's or processor's retention period.
- (f) Data protection impact assessments should be carried out where a processing operation is likely to result in a high risk to the rights and freedoms of a data subject. The General Regulations set out which processing activities will require the carrying out of an impact assessment (see question 6.3).
- (g) Comprehensive recordkeeping of processing activities should form part of the internal processes implemented by data controllers and data processors in order to ensure compliance with the DPA. This is particularly important where an audit is carried out by the ODPC.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The obligations under the DPA largely apply equally to both data controllers and data processors. For instance, both controllers and processors are required to register with the ODPC. If the same entity acts as both a controller and processor, two separate registrations must be in place.

However, data controllers and data processors have different reporting requirements under the DPA that must be complied with in the event of a breach. The controller is required to notify and communicate the breach to the ODPC and to the data subject in the prescribed instances. A data processor, on the other hand, is required to notify only the data controller, without delay and, where reasonably practicable, within 48 hours of becoming aware of a breach.

The DPA further requires that a data processing agreement must be entered into where a data controller uses the services of a data processor, with the General Regulations prescribing the provisions to be included in such an agreement.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, the DPA requires a lawful basis to be relied upon to process personal data. A data controller or processor may only process personal data if the data subject has given consent to its processing, or where one of the other grounds set out below is relied upon to process personal data. The data must then be used or processed solely for the purpose for which it was collected: failure to do so amounts to an offence.

The processing of personal data can only be done without the data subject's consent where the processing is necessary for one of the following reasons:

- (a) for the performance of a contract to which the data subject is a party in order to take steps at the request of the data subject before entering into a contract;
- (b) for compliance with a legal obligation to which a controller is subject;
- (c) to protect vital interests of the data subject or another natural person;
- (d) for public interest or in the exercise of official authority vested in the controller;
- (e) for the performance of any task carried out by public authorities;
- (f) to pursue legitimate interests unless the processing is unwarranted due to potential harm or prejudice to the data subject's rights, freedoms, or legitimate interests, or
- (g) for historical, statistical, journalistic, literary, artistic, or scientific research.

The General Regulations further clarify that only one legal basis may be relied upon at a time, and it must be identified before processing begins. Additionally, data controllers must be able to demonstrate the legal basis relied upon at all times where the controller uses multiple bases for different processing.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Kenyan law does not specify a particular type of notice for processing data for advertising. However, the General Regulations and the DPA require that data subjects be clearly informed of the data controller's or processor's identity, contact details, and the purpose of processing the relevant personal data. Personal data, other than sensitive personal data, may be used for direct marketing where the data subject provides informed consent for its use or disclosure for the purpose of direct marketing. Any intent to share this personal data with third parties must be disclosed through a privacy notice or policy, and sufficient data protection safeguards adopted. However, personal data may be collected indirectly where the data subject has consented to its collection from another source.

Moreover, under the General Regulations, companies must develop, publish and regularly update a policy reflecting their personal data handling practices. The policy should include the following information:

- (a) the nature of the personal data collected and held;
- (b) the lawful purpose for data processing;
- (c) how a data subject can access their data and exercise their rights;
- (d) the complaints handling mechanism, including a process for individuals to raise concerns or complaints regarding how their data is used;
- (e) international data transfers, including the recipients and any safeguards in place to protect the data;
- (f) data retention provisions, indicating how long personal data will be stored before it is deleted or anonymized; and
- (g) processing of children's data, including how data from minors is collected and the safeguards in place to ensure compliance with child data protection standards.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Under the Constitution, every person has the right of privacy, which includes the right not to have information about their family or private affairs unnecessarily requested or revealed, or the privacy of their communications infringed. This right has been reiterated in several decisions by the High Court and there have been several successful claims before the High Court on the protection of the constitutional right to privacy.

Under the DPA, individuals including consumers have the right:

- (a) to be informed about the use to which personal data is to be put;
- (b) to access their personal data in the custody of the data controller or processor;
- (c) to object to the processing of their personal data;
- (d) to correction of false or misleading data; and
- (e) to the erasure of false or misleading data.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Data controllers and data processors must always obtain the consent of data subjects to use their personal information for commercial purposes including advertising. They must also always provide for the option to opt out of direct marketing communications, and such option must be free and simple.

Opt-out messages or mechanisms must:

- (a) be visible, clear and provide an easily understood explanation of how to opt out;
- (b) require minimal time and effort;
- (c) provide a direct and accessible communication channel;
- (d) be free of charge or involve a nominal cost where necessary; and
- (e) be accessible for persons with disabilities.

Further, when a company lawfully obtains a customer's email address or phone number during the sale of a product or service, it is permitted to use these details for direct marketing—but only for products or services that are similar to what the customer originally purchased. Businesses are required to offer customers a clear, simple, and free option to opt out of receiving such messages. This opportunity must be provided at the time of data collection and in every subsequent marketing message if the customer did not initially opt out. This ensures that consumers retain control over their personal information and are not subjected to unwanted marketing communications.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The DPA sets out matters to be considered when using personal data for commercial purposes (see question 4.1). Additionally:

- (a) Vendors cannot transfer any personal data to a third party without the consent of the data subject;
- (b) Data controllers must select a data processor with adequate organizational safeguards and enter into a written contract which binds the processor to act only on the controller's instructions and adhere to the controller's obligations;

- (c) Parties involved in sending and receiving the data should enter into a written data-sharing agreement, ensuring that the third party adheres to the same data protection standards and principles as mandated by the DPA; and
- (d) Data processors are prohibited from engaging with third parties without the prior authorization of the data controller.

6.2 **What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?**

The DPA mandates that routine sharing of personal data between entities be governed by formal data sharing agreements. These agreements serve to clarify the roles and responsibilities of each party and to ensure adherence to data protection principles. The key elements that should be included in a data sharing agreement include the duties of each party, implementation of data security measures, compliance with data subject rights and breach notification procedures.

Both the disclosing and receiving entities should have specific responsibilities to ensure compliance with the DPA:

- (a) The disclosing entity must ensure that the data sharing is justified, lawful, and that all data subjects are informed about how their data will be used and shared.
- (b) The receiving entity should be required to implement adequate safeguards to protect the shared data, use it only for the specified purposes, and uphold the rights of data subjects. They must also ensure that any further sharing of the data complies with the original data sharing agreement and all applicable laws.

6.3 **What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?**

Companies are expected to conduct a periodic review of their data processing activities to ensure compliance with the DPA. In addition, due diligence should be undertaken on any data processors engaged by a data controller to ensure that they comply with the provisions of the DPA.

As regards the requirements for a data protection impact assessment ('DPIA'), the DPA requires data controllers and processors to conduct a DPIA prior to initiating any processing operations likely to result in high risks to data subjects. The DPIA should include a detailed analysis of potential risks and the measures implemented to mitigate them. In 2023, the ODPC provided a Guidance Note on Data Protection Impact Assessment ('Guidance Note') to assist organizations in this process. The Guidance Note outlines the following to be considered in order to determine which set of processing operations require a DPIA:

- (a) personal data that concerns vulnerable data subjects such as children, minorities or persons with disabilities;
- (b) processing that involves automated decisions impacting individuals' legal rights or similar significant effects;
- (c) processing that involves regular and systematic observation of individuals, especially in public areas;
- (d) processing of sensitive personal data;
- (e) large-scale data processing;
- (f) data processing that employs the use of new technologies; or
- (g) processing that may restrict subjects from exercising their rights over their personal data.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The DPA requires the data controller or processor to obtain the consent of the data subject before processing personal data for commercial purposes. The DPA and its Regulations provide for the manner in which personal data can be used for commercial purposes, including for direct marketing purposes. Sensitive personal data cannot be used for commercial purposes. Prior to using personal data for direct marketing, it is necessary to obtain the consent of the data subject and ensure that all communications include a simplified opt-out mechanism. Direct marketing activities that are regulated under the General Regulations include the display of advertisements through online media platforms.

The data subject has the right to object to the processing (which can include any profiling to the extent necessary) of personal data for any commercial use. Where the data subject objects, their personal data cannot be processed for any commercial use.

As to the key considerations and offenses related to direct marketing when a company lawfully obtains a customer's email address or phone number during the sale of a product or service see question 5.3.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies or any form of profiling must be carried out in accordance with the DPA if it generates any form of identifiers from which a person can be identified directly or indirectly (as this would constitute personal data and possibly sensitive personal data). The General Regulations also recognize that personal data may be collected indirectly from information associated with web browsing, which we consider may apply to cookies. Where personal data is collected indirectly, the data controller or data processor should, within 14 days, inform the data subject of the collection. Aside from this, there are no additional express provisions or restrictions which prohibit or otherwise govern the use of tracking technologies under Kenyan law.

7.3 How are loyalty programs and promotions regulated under privacy law?

The primary legislation that regulates loyalty programs and promotions in Kenya is the Betting Gaming and Lotteries Act, which does not touch on privacy issues. However, although there is no specific regulation of loyalty programs and promotions from a privacy perspective, the DPA would apply where such programs collect personal data, and, in particular, sensitive personal data (which can include property details and marital details).

7.4 How is social media and influencer marketing regulated under privacy law?

Kenyan law does not have specific provisions on the regulation of social media companies. However, social media companies would be required to ensure that users' right to privacy is protected under the Constitution. There was an attempt to introduce a Social Media Bill in 2019, which proposed to introduce stringent regulation of use of social media in the country. The Bill sought to license social media companies by requiring them, inter alia, to keep all the data of the users of their platforms and submit this to the Communications Authority of Kenya when required. However, the Bill has now lapsed.

Influencer marketing often involves collaborations with individuals who have a significant online following to promote their products or services, making it a unique subset of social media marketing.

Influencer marketing often involves sponsored posts, product placements, or brand partnerships on social media platforms. However, the DPA and its Regulations do not have specific provisions on the regulation of influencer marketing.

Additionally, the Code of Advertising Practice and Direct Marketing published by the Advertising Standards Body of Kenya ('ASBK') regulates the use of testimonials in advertising, which applies to influencer marketing. The Code applies to advertisers, advertising practitioners, facilitators providing data and statistics, and media platforms involved in publishing or broadcasting advertisements. It provides that any testimonials and endorsements in advertisements must be genuine, based on personal experience over a reasonable period, and not rely on third-party opinions. Outdated or misleading testimonials, as well as claims of efficacy that cannot be substantiated, are prohibited. Moreover, any 'before' and 'after' claims must allow fair comparison, and any conflicting statements can only be amended with the written approval of the ASBK.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Since the displaying of an advertisement on an online media platform where the data subject is logged on using their personal data is categorized as direct marketing, the General Regulations should be considered in the context of targeted advertising. Additionally, all targeted or behavioral advertising has to comply with the constitutional right to privacy and the DPA (particularly insofar as any such forms of advertising may amount to profiling and where this may include sensitive personal information). With this in mind, the use of any personal data collected must be limited to the purposes for which it was collected.

Contextual advertising, on the other hand, delivers ads based on the content of the webpage a user is viewing rather than their personal data. This form of advertising is not subject to the requirements applicable to targeted advertising, since it does not require the tracking of individual user behavior, nor does it place reliance on collected personal data. It is important to note, however, that the DPA places no distinction between the two.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Whilst these two concepts have a direct impact on data subject privacy, Kenya does not have a specific legal framework governing digital identity resolutions and clean room technologies. However, where the use of these technologies is likely to result in a risk to a data subject, DPIAs should be carried out to identify and mitigate any possible risks and ensure that there are sufficient safeguards to protect personal data.

7.7 How is location-based advertising regulated under privacy law?

Specific provisions on location-based advertising do not exist within the Kenyan privacy legal framework. However, information on a data subject's geographical location is personal data.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific privacy rules governing data brokers; however, a data controller who, without lawful reason, discloses personal data in any manner that is incompatible with the purpose for which the data was collected contravenes the DPA. Moreover, any person who offers to sell personal data where the data has been obtained unlawfully (ie, in a manner that is incompatible with the purpose of

collection) commits an offense. An advertisement indicating that personal data is, or may be, for sale constitutes an offer to sell the personal data under the DPA.

The definitions of ‘data processor’ and ‘data controller’ under the DPA are broad and would include data brokers in their ambit.

7.9 How is advertising to children and minors regulated under privacy law?

Processing a child’s data requires parental or guardian consent. However, organizations providing counseling or child protection services exclusively to children may be exempt from this requirement.

Processing must be conducted in a way that protects the child’s rights and best interests. Thus, even when a duly authorized person exercises a child’s data rights, data controllers and processors must act in the best interests of the child. Profiling children for direct marketing is prohibited, and parents or guardians must be informed of the risks and safeguards involved in data processing. If uncertainty arises regarding the relationship between the authorized person and the child, data controllers or processors may restrict the exercise of rights until proper verification is provided.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Data subjects have the right not to be subjected to a decision based solely on automated processing, including profiling, unless:

- (a) it is necessary for the performance of the contract between the data subject and data controller,
- (b) it has been authorized by law that contains suitable data protection safeguards to which the data controller is subject, or
- (c) consent has been given by the data subject.

The use of artificial intelligence technologies is not specifically regulated under the DPA.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The DPA does not bar the transfer of data outside Kenya. However, according to the Data Protection Principles, every data controller or processor must ensure that personal data is not transferred outside of Kenya unless there is proof of adequate data protection safeguards, or the data subject has consented to such transfer.

Additionally, the DPA sets out conditions that must be met before data is transferred outside Kenya. Accordingly, a data controller or data processor may transfer personal data to another country only where:

- (a) it has given proof to the ODPC of the appropriate safeguards with respect to security and protection of the personal data;

- (b) it has given proof to the ODPC of the appropriate safeguards, which include ensuring that the jurisdictions to which data is being transferred have commensurate data protection laws; or
- (c) the transfer is necessary for:
 - (i) performance of a contract between the data subject and the data controller or data processor;
 - (ii) the conclusion or performance of a contract in the interest of the data subject between the controller and another person;
 - (iii) any matter of public interest;
 - (iv) establishment, exercise or defense of a legal claim;
 - (v) protection of the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
 - (vi) compelling legitimate interests pursued by the data controller or data processor that are not overridden by the interests, rights and freedom of the data subject.

In the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity being met, cross-border transfers can be effected only with the explicit consent of the data subject where the data subject has been informed of the possible risks of such transfer.

Adequacy decisions are yet to be published; however, the General Regulations recognize that 'appropriate safeguards' include contractual binding rules among a concerned group of undertakings or enterprises. Sensitive personal data may only be processed outside Kenya upon obtaining the prior consent of the data subject and upon obtaining confirmation of appropriate safeguards in the receiving jurisdiction. The onus will be on the data controller or processor to show that appropriate safeguards are in place. The ODPC may request the data controller or data processor transferring personal data out of Kenya to demonstrate the effectiveness of the safeguards or existence of compelling legitimate interests. Under the DPA, the ODPC is further entitled to prohibit, suspend or subject the transfer to such conditions as may be determined.

8.2 **Are there any additional considerations for personal data transfers (eg, privilege concerns)?**

In certain instances, the Cabinet Secretary for Information, Communications and Technology may, on grounds of strategic interests of the State or protection of revenue, prescribe that certain types of processing only be effected through a server or data center located in Kenya.

The General Regulations indicate that where personal data is to be transferred between a group of companies outside Kenya, appropriate data protection safeguards must exist to ensure that the level of protection accorded by the DPA is not undermined. In order to confirm the existence of appropriate data protection safeguards within multinationals, there must exist contractual binding corporate rules ('BCRs') among the group of companies concerned.

9 **DATA SECURITY AND BREACH MANAGEMENT**

9.1 **How is data security regulated in Kenya? Are there minimum standards? Does this differ by sector or size of the entity?**

- (a) The DPA contains provisions for regulation of data breaches but has not expressly provided for any minimum standard for securing data. The DPA only specifies that the technical and organizational measures to be implemented must take into consideration:

- (i) the amount of personal data collected,
- (ii) the extent of the processing,
- (iii) the period of storage,
- (iv) the accessibility of such data,
- (v) the cost of processing data and
- (vi) the technologies and tools used.

Furthermore, as part of the registration process, the application to the ODPC must include a general description of the risks, safeguards, security measures and mechanisms in place to ensure the protection of personal data.

- (b) The regulation of the banking and financial services sector is stricter in relation to how regulated entities are required to protect their data. The Central Bank of Kenya has published guidelines that serve as the minimum standard that banks and payment service providers should adopt when dealing with the security of their data.

9.2 How are personal data breaches regulated in Kenya? What are the requirements for notification and response?

The DPA defines a ‘personal data breach’ as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of, or access to, personal data transmitted, stored or otherwise processed.

Where the data processor becomes aware of the breach, it must communicate such fact to the data controller within 48 hours upon becoming aware of the breach. Data controllers must communicate the breach to the ODPC within 72 hours of becoming aware of the breach, and communicate the breach to the data subject in writing within a reasonable period, unless the identity of the data subject cannot be traced. However, the data controller is not required to communicate the breach to the data subject where appropriate security safeguards have been implemented. These safeguards may include the encryption of affected personal data.

The data controller may delay or restrict its communication to the data subject or to the ODPC as necessary for the purpose of preventing, detecting or investigating an offence by a concerned or relevant body.

The communication to the ODPC and data subject should contain, among other things, a description of the nature of the breach, description of measures taken to address the breach, and recommendation of measures the data subject should take to mitigate the effects of the data compromise, as well as a contact point should the ODPC or data subject require further information.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) The following penalties apply for non-compliance with the DPA:
 - (i) An administrative penalty of up to KES 5 million (USD 50,000) or, in the case of an undertaking, up to 1% of annual turnover, whichever is the lower;
 - (ii) For obstructing the ODPC in the exercise of its powers, failure to provide information or assistance, denying entry to the ODPC or giving the ODPC false or misleading information, a fine not exceeding KES 5 million (USD 50,000) or imprisonment for a term not exceeding two years or both.

- (iii) For failure to comply with an enforcement notice, a fine of up to KES 5 million (USD 50,000) or imprisonment for a term not exceeding two years or both.
- (iv) It is an offense for a data controller to disclose personal information without any lawful reason and in any manner incompatible with the purposes for which the data has been collected. It is also an offense for a data processor, without lawful reason, to disclose personal data processed by the data processor, without the prior authority of the data controller.
Further, it is an offense for a person to obtain access to personal data, or to obtain information constituting such data, without prior authority of the data controller or processor, or to disclose personal data to third party.
The DPA criminalizes any offer to sell personal data/any advertisement to sell personal data.
- (v) For an offense where no specific penalty has been provided, a fine not exceeding KES 3 million (US \$30,000) or imprisonment to a term not exceeding 10 years or both. In addition, the Court may, in order to prevent a contravention continuing, order forfeiture of equipment used in committing the offense or prohibit any act related to the contravention.
- (vi) Any person who suffers damage as a result of infringement of the provisions of the DPA is entitled to damages from the data controller or processor.
- (b) Under the Kenya Information and Communications Act,
 - (i) any person who gains access to a computer system for the purpose of securing a service or intercepts a function of, or any data within a computer system is guilty of an offense, punishable upon conviction with imprisonment for a term not exceeding three years or a fine not exceeding KES 500,000 (US \$5,000) or both. Furthermore, if, during the commission of the offense, data is suppressed or impaired, the penalty is a fine not exceeding KES 200,000 (US \$2,000) or imprisonment for a term not exceeding two years or both.
 - (ii) any person who knowingly discloses a password to access a computer system for unlawful gain commits an offence, punishable with a fine not exceeding KES 200,000 (US \$2,000) or imprisonment for a term not exceeding two years or both.
- (c) Under the HIV& AIDS Prevention and Control Act, any person who discloses the HIV test results of another person without their consent commits an offense, punishable upon conviction with a fine not exceeding KES 100,000 (USD 1,000) or imprisonment for a term not exceeding two years or both.

10.2 Do consumers have a private right of action? What remedies are available to them?

- (a) Under the Constitution, every person has the right to institute proceedings alleging breach of constitutional rights. If the right of privacy is infringed upon, one can institute a claim in the High Court. The High Court can grant remedies such as a declaration of rights, an injunction, a conservatory order and a declaration of invalidity of a law, an order for compensation and order for judicial review.
- (b) Under the DPA, an individual can lodge a complaint with the ODPC, which may investigate the complaint. Where the ODPC is unable to obtain an amicable solution, it must notify the complainant in writing. A person who suffers damage because of contravention of the DPA is entitled to compensation from the data controller or data processor.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The ODPC is very active in enforcing the right to privacy and other privacy related provisions. This can be seen from the examples below:

- (a) In the 2024 decision of *Victory Owino v Wananchi Group (K) Ltd, ODPC Complaint No 1992 of 2023*, Wananchi Group Limited, trading in Kenya as Zuku, was ordered to pay an ex-customer KES 250,000 (approx USD1,930) for sending the complainant promotional messages without her consent and continuing to send the promotional messages despite her refusal and requests to delete her details from the company's system.
- (b) In the 2025 decision of *Yasin Abukar v Wananchi Group (Kenya Limited, ODPC Complaint No 1880 of 2024*, Zuku was fined a further KES 500,000 (approx USD 3,860) for another privacy breach. Zuku failed to delete the data of the complainant (a former customer) in their possession and ignored his requests to stop sending him promotional messages. The company was additionally ordered to delete his data within seven days. The ODPC has recommended that the directors of Zuku be prosecuted for obstruction after ODPC officers were blocked from accessing relevant records.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Kenya?

There are currently no laws particular to Kenyan culture that affect privacy.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

- (a) The ODPC has issued further regulations, guidance or codes in relation to the implementation and application of the DPA.
- (b) The Proposed Co-regulation Framework for Broadcast and Over The Top/Video On Demand Content: The Kenya Film Classification Board ('KFCB') proposes to introduce this framework, which will require VOD and OTT service providers to self-classify any content intended to be broadcast and ensure they meet the filming license requirements. As currently drafted, the Co-Regulation Framework only applies to entities operating in Kenya, and that have a presence in Kenya. Public consultations were conducted in 2022, and the framework is pending finalization and implementation.
- (c) The Film Bill 2021, if enacted, will consolidate the legislative framework of laws relating to the film industry, provide for the establishment, powers and functions of the film industry entities and provide for the development, funding and regulation of the film industry. From a privacy perspective, the Bill proposes to regulate content service providers by expanding the functions of KFCB to include regulating the creation, broadcasting, distribution, possession and exhibition of films by:
 - (i) advising on and promoting the consumption of classified films online in order to protect the safety of women, children and other vulnerable members of society against sexual exploitation or degradation and safeguarding their privacy and identity in film content;
 - (ii) alerting online content service providers about unclassified films being exhibited on their platforms; and

- (iii) advising the Communications Authority of Kenya to issue compliance notices to Internet Service Providers for unclassified films being exhibited on the platforms of the online content service providers.
- (d) Industry Guidelines for Child Online Protection and Safety in Kenya ('COP Guidelines') developed by the Communications Authority seek to introduce a set of organizational and technical standards and regulations for social media service providers by requiring them to develop and publicize the processes for handling of complaints and enquiries on online violation of children's rights (eg, child sexual abuse material, inappropriate content or contact, breaches of privacy etc), and adapt and implement heightened default privacy settings for the collection, processing, storage, sale and publishing of personal data, including location-related information and browsing habits, gathered from people under 18 years. They provide a basis for the design, development, deployment, commissioning, use, management, sale, marketing and publicity of communication products and services in Kenya that may be accessed and/or targeted for use by children; and safeguards for children's access to and use of ICT services in Kenya. Since the introduction of the COP Guidelines, there has been ongoing collaboration between the government, industry stakeholders, and civil society to ensure effective implementation and adherence to these protective measures.
- (e) In 2024, the ODPC developed a draft Data Sharing Code and draft Data Protection (Conduct of Compliance Audit) Regulations. The Code outlines key principles such as lawfulness, fairness, transparency, and data minimization. It emphasizes the need for data sharing agreements, the importance of assessing the legal basis for sharing, and the implementation of robust security measures. It also addresses specific scenarios like data sharing in emergency situations and cross-border data transfers, providing a comprehensive framework for entities engaged in data sharing activities. The Regulations will empower the OPDC to initiate compliance audits on data controllers and processors to assess their conformity with data protection laws. These audits can be periodic or triggered by specific incidents, such as data breaches or complaints.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Currently, there has been an increase in conversations concerning Artificial Intelligence ('AI') and its implications across various industries, which can encompass the use of AI in advertising. The integration of AI in advertising will reshape how brands interact with consumers, personalize content, and optimize marketing campaigns. However, with AI being capable of collecting and processing vast amounts of consumer data, the advancement of AI in the advertising space sparks regulatory concerns, particularly in the areas of data privacy, transparency, and ethical advertising.

Another area of concern is the risk of AI-generated misinformation and deceptive advertising. AI tools will become more sophisticated in creating realistic images, videos, and even deepfake content. Therefore, there is increasing pressure on regulators to establish clear guidelines on the responsible

use of AI in advertising. The Media Council of Kenya has also recently formed a technical committee to develop ethical guidelines on AI application in media and, potentially, advertising. In 2025, the committee released several key documents:

- (a) Data Governance Guide for Media Practice in Kenya;
- (b) Media Handbook for Reporting on Artificial Intelligence in Kenya;
- (c) Media Guide on the Use of Artificial Intelligence in Kenya; and
- (d) Guide on the Use of Social Media and the Internet for Media Practice in Kenya

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

- (a) **Data breaches:** In the process of transitioning from analogue data storage systems to digital systems, there have been instances where companies have suffered significant data breaches. Lack of appreciation of the required security and technical safeguards is a contributory factor.
- (b) **Increase in regulatory burden and associated costs:** Regulation of data is increasing as companies are coming to terms with the changed legal landscape and the necessity to ensure they comply with the local privacy laws. While international companies may be more accustomed to compliance with the EU GDPR, local companies will have to ensure that sufficient time and money are allocated towards ensuring compliance with the DPA.

- (c) **Litigation risk:** Owing to an increase in regulation, companies will find themselves before the courts over breach of privacy issues. There have already been instances where litigants have sought to protect their constitutional rights before the courts. For example, a well-known university in Kenya was sued for testing and revealing the results of the HIV test of one of its employees without her consent. The Complaints Regulations clearly set out the procedure by which the ODPC should handle complaints once presented either by the data subject or by a third party.

Moreover, the ODPC has imposed significant penalties on entities that fail to adhere to data protection laws such as using individuals' images without consent. A private educational institution in Kenya was fined KES 4,550,000 (approx USD 35,150) for posting images of minors on social media without obtaining consent from their parents or guardians, thereby reinforcing the principle that children's data must be handled with extra caution to protect their privacy and rights.

Similarly, an individual who had visited a popular entertainment establishment, discovered their image being used for promotional purposes without prior approval. The lounge was penalized KES 1,850,000 (approx USD 14,300) for using a patron's image on its social media platforms without their consent. In September 2023, the ODPC announced three penalties totaling KES 9,375,000 (approx USD 72,430) for alleged violations of the Data Protection Act.

- (d) **Data Localization:** The General Regulations provide that, where data processing is done for the purpose of strategic interests of the State, the processing should be effected through a server and data center located in Kenya, or at least one accessible copy of the personal data should be stored in a data center in Kenya. 'Strategic interests of the State' have been described to include:
 - (i) providing primary or secondary health care for a data subject in the country;
 - (ii) offering early childhood education and basic education; and
 - (iii) running a system designated as a protected computer system under the Computer Misuse and Cybercrime Act 2018.

12.3 What do you envision the privacy landscape will look like in five years?

Given the current trajectory of the landscape, we envision that privacy in Kenya will be subject to stricter regulation due to a growing appreciation of the need for regulation and protection of information. This will also bring about certainty in terms of the rights and compliance obligations of data controllers and data processors. Additionally, access to internet and data services, as well as the development and use of AI, is expected to continue to grow, and we anticipate added growth in the number of companies offering e-commerce services.

We anticipate that emerging technologies such as AI and biometric systems will prompt the ODPC to develop new regulations and guidelines, while sector-specific laws may be introduced to address privacy concerns in areas like fintech and cryptocurrencies, healthcare, and telecommunications.

 MALAYSIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Malaysia.

Privacy in Malaysia is regulated primarily under the Personal Data Protection Act 2010 ('PDPA'), which governs the collection, use, storage, and transfer of personal data. The PDPA applies to organizations in Malaysia that process or have control over or authorize the processing of personal data in connection with commercial transactions. The PDPA outlines principles for the protection of personal data, including the need for consent, purpose limitation, accuracy, security, and access rights.

1.2 What are the primary laws regulating privacy in Malaysia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy in Malaysia is regulated primarily under the PDPA. Other relevant legislation include:

- (a) The General Code of Practice of Personal Data Protection, which complements the PDPA by providing more detailed guidelines on best practices for organizations when processing personal data which includes specific provisions on consent management, data security, and data retention practices;
- (b) Communications and Multimedia Act 1998, which governs the collection and disclosure of personal data through telecommunication services, and includes provisions that affect privacy in the context of online services, mobile services, and internet service providers; and
- (c) Financial Services Act 2013, which imposes specific privacy and confidentiality obligations on financial institutions to protect customer data and prevent unauthorized disclosure.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation complements the framework under the PDPA by providing additional standards and guidelines that advertisers can follow. For example, while the PDPA requires organizations to obtain consent before collecting or using personal data, advertisers can offer more detailed guidelines about transparency in targeted advertising, such as providing easy-to-understand privacy notices or allowing users more control over their data through opt-out mechanisms.

Self-regulation is often achieved through the adoption of industry codes of conduct and guidelines which set out best practices that organizations within the advertising sector are encouraged to follow.

The Malaysian Digital Association, a key industry body, often provides guidelines on digital advertising practices, encouraging advertisers to protect consumer privacy.

1.4 How is privacy law enforced in Malaysia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy law is enforced by the Personal Data Protection Commissioner ('PDPC'), which is the regulatory authority established under the PDPA, and by the public at large. The PDPC is responsible for ensuring compliance with the PDPA, investigating complaints, and taking enforcement actions against violators. Any individual or relevant person may make a complaint in writing to the PDPC, who will then investigate the matter. Investigation may continue despite withdrawal of the initial complaint. If a data user is found to have contravened any provisions of the PDPA after investigation

is completed, the PDPC may issue an enforcement notice outlining directions to be complied with by the data user. Besides fines and criminal sanctions, the PDPC can issue warning notices or demand that organizations undertake corrective actions.

Additionally, self-regulatory bodies also play a key role in privacy law enforcement in Malaysia, especially in sectors such as advertising and digital marketing. These bodies, such as the Malaysian Digital Association and the Advertising Standards Authority Malaysia, create and promote industry standards for data protection. These self-regulatory bodies do not have the legal authority to issue penalties for non-compliance; instead, their functions are complementary to the legal enforcement undertaken by the PDPC.

Under the PDPA, individuals also have the right to pursue private actions against organizations if they have suffered loss or damage as a result of non-compliance with the PDPA. The Malaysian courts may grant remedies such as damages or an injunction, requiring the organization to take specific actions to correct the violation.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Malaysia?

A company is subject to privacy law in Malaysia if it collects personal data to be processed or to be further processed in relation to commercial transactions in Malaysia.

2.2 Does privacy law in Malaysia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Malaysian privacy law applies if the foreign company collects personal data which is to be processed or is intended to be further processed in Malaysia.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Malaysia?

‘Personal data’ means any information in respect of commercial transaction, that relates directly or indirectly to a data subject and expression of opinion about the data subject, which:

- (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive personal data’ includes any personal data consisting of information as to the physical or mental health or condition of a data subject, their political opinions, racial or ethnic origin, criminal record or allegation of criminal activity, religious beliefs or other belief of a similar nature, the commission or alleged commission by them of any offence, or any other personal data as the Minister may determine by order published in the Gazette.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized data is not considered personal data under the PDPA since the data has been processed in such a way, by stripping of all personally identifiable information (such as names, addresses, or contact numbers), that it can no longer identify an individual, either directly or indirectly.

Pseudonymization is a process that replaces personally identifiable information with artificial identifiers or pseudonyms. Although the likelihood of identifying an individual without additional information is reduced, the data is still capable of being re-identified through other means. Therefore, the PDPA's obligations for personal data would still apply.

De-identified data is data that has been processed to remove personally identifiable information. Such data is often treated similarly to anonymized data in that it may not be considered personal data, provided that it cannot reasonably be re-identified. If the data remains identifiable through the use of additional data or other means, it is still subject to the PDPA.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The key principles that organizations should follow when processing personal data under the PDPA are:

- (a) Personal data must be processed fairly and lawfully, with the individual's consent;
- (b) Organizations must inform individuals of the purpose for which their data is being collected before collecting it. They must provide clear notice to the individual regarding the data collection and processing;
- (c) Personal data must not be disclosed to third parties without the consent of the individual, unless required by law or when it is necessary for business operations;
- (d) Organizations must take appropriate security measures to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, or destruction;
- (e) Personal data should not be kept longer than necessary for the purpose for which it was collected;
- (f) Personal data must be accurate, complete, and up-to-date;
- (g) Individuals have the right to access their personal data held by organizations and request corrections if the data is inaccurate or incomplete; and
- (h) Individuals have the right to request that their personal data be transmitted to another data user of their choice, subject to technical feasibility and compatibility of data format (ie, data portability).

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

There are no specific roles assigned in companies in relation to processing of personal data. However, the law defines 'data processor' and 'data user' as follows:

- (a) 'Data processor', in relation to personal data, means any organization/person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes;

- (b) 'Data user' means an organization/person who either alone or jointly or in common with other organizations/persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.

As the primary party responsible for the personal data, the data user holds ultimate responsibility for ensuring compliance with all aspects of the PDPA. The processor has fewer direct obligations under the PDPA, but is still required to follow the data user's instructions and ensure appropriate security measures are in place.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The PDPA generally requires that organizations process personal data only if they have a lawful basis for processing personal data, with consent being the most commonly used lawful basis. Organizations can rely on other bases, such as contractual necessity, legal obligations, and public interest, depending on the situation.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

When preparing a privacy notice for advertising purposes, organizations are required to inform individuals of specific details regarding the processing of their personal data. Such notices must include clear explanations of the purposes for which personal data will be used, rights of individuals, third-party disclosures, data retention practices, and security measures, among other details. It is also important that contact information for individuals to direct inquiries related to their personal data processing is provided.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

There are three rights of data subjects, namely:

- (a) **Right to access to personal data:** an individual is entitled to be informed by a data user whether their personal data is being processed by or on behalf of the data user;
- (b) **Right to correct personal data:** a data subject may make a data correction request in writing to the data user if the data subject knows that the personal data being held by the data user about them is inaccurate, incomplete, misleading or not up-to-date; and
- (c) **Right to withdraw consent to process personal data:** a data subject may, by notice in writing, withdraw consent to the processing of their personal data.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Organizations must obtain consent from individuals before collecting their personal data for the purpose of advertising. The organization must clearly inform individuals of the purpose for collecting their personal data and how the data will be used. There must be an easy and accessible mechanism for consumers to opt out of advertising activities, such as unsubscribe links in emails or stop options in SMS messages.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Under the PDPA, the organization collecting or controlling the personal data (ie, the data user) remains responsible for ensuring that personal data is handled in compliance with the PDPA, even when third parties or vendors are involved. The data user must ensure that third parties follow strict data protection standards through contracts, consent, and monitoring. Additionally, organizations must ensure transparency, security, and appropriate safeguards when sharing personal data with third-party vendors, particularly in advertising practices.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The contractual obligations must ensure compliance with PDPA's data protection principles (see question 4.1). The contract should also contain a confidentiality clause ensuring that the third party or vendor keeps the personal data confidential and does not disclose it to unauthorized parties. Vendors must be obligated to notify the data user promptly if there is any data breach or security incident involving personal data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Most importantly, organizations should ensure that their privacy practices comply with the various obligations under the PDPA (see question 4.1).

Organizations must conduct impact assessments when their activities, such as advertising or marketing campaigns, involve high risks to the privacy rights of individuals. Such assessments help assess the impact of planned data processing on personal privacy, and identify measures to mitigate those risks. Impact assessments can be conducted when creating new systems/processes involving handling of personal data, or when changing the way in which existing systems/processes handle personal data (eg, new database/portal).

Impact assessments ideally identify how data flows through system/process so as to identify risks and enable implementation of security measures addressing risks.

Vendors should perform due diligence on third-party vendors (eg, advertising agencies, data brokers, cloud service providers) which handle personal data by ensuring that vendors comply with the PDPA and provide adequate data protection safeguards.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing is tightly regulated under the PDPA and the Communications and Multimedia Act 1998. An individual may, at any time, notify the organization to cease or not to begin processing their personal data for marketing communications. Organizations are obliged to comply with such requests, and they must cease the use of personal data for marketing purposes once a valid request has been

made. If the organization fails to comply with the notice, the individual may submit an application to the PDPC to require the data user to comply with the notice. The PDPC may then require the organization to comply with the notice and if this fails, the organization may face regulatory actions, penalties, or fines.

Organizations must provide a simple and accessible means for individuals to opt-out or unsubscribe from receiving marketing communications. This includes providing an option to unsubscribe from mailing lists or opting out of marketing campaigns in any electronic communication.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Under the PDPA, the use of tracking technologies is subject to the same principles that govern the processing of personal data. A service provider may collect and maintain necessary data or information of a data subject for tracking practices. However, the collection and maintenance of such data or information must follow good practices, namely it must be:

- (a) fairly and lawfully collected and processed;
- (b) processed for limited purposes;
- (c) adequate, relevant and not excessive;
- (d) accurate;
- (e) not kept longer than necessary;
- (f) processed in accordance with the data subject's rights;
- (g) secure; and
- (h) not transferred to any party without prior approval from the data subject.

7.3 How are loyalty programs and promotions regulated under privacy law?

The use, collection and process of personal data must be in accordance with the PDPA. Transfer of personal data to a third party or places outside Malaysia must be done with the prior consent of the data subject.

7.4 How is social media and influencer marketing regulated under privacy law?

The use, collection and process of personal data must be in accordance with the PDPA. The PDPA aims to protect individuals' privacy while allowing businesses to leverage social media platforms for marketing purposes. Transfer of personal data to a third party or to countries outside Malaysia must be done with the prior consent of the data subject. Individuals should have the option to opt-out of direct marketing activities.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Generally, targeted advertising and behavioral advertising must be in accordance with the PDPA (see question 4.1).

Targeted advertising (including behavioral and personalized advertising) is subject to strict regulations under the PDPA, particularly around consent, transparency, and data protection practices.

Contextual advertising, in contrast to targeted advertising, delivers advertisements based on the content of the website or application being viewed rather than on personal data. Since contextual advertising does not rely on personal data but rather on the context in which the user is interacting with content, it generally does not require the same level of scrutiny under the PDPA as targeted

advertising. As long as no personal data is being collected, used, or disclosed for the purpose of delivering the advertisement, the PDPA may not apply in the same way. However, if any personal data is collected indirectly (such as through cookies or device identifiers), consent would still be required under the PDPA.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution, which refers to the process of combining data from multiple sources (both online and offline) to create a more complete profile of an individual, and clean room technologies, which refers to a secure environment where multiple organizations or entities can aggregate and analyze data without exposing raw personal data to any party, often involve the use of personal data for various purposes, including targeted advertising, data analytics, and audience segmentation. Both technologies will need to comply with the obligations under the PDPA (see question 4.1).

Additionally, with respect to data clean rooms, to minimize re-identification of individuals from personal data, the use of data anonymization or pseudonymization techniques is important. This ensures that the data shared within the clean room cannot be traced back to individuals. If third-parties are involved, organizations must ensure that these third parties are compliant with the PDPA.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is regulated under the PDPA and would need to comply with the various obligations under that Act (see question 4.1), as it involves the collection of personal data that can identify or track individuals. ‘Personal data’ can include location data (eg, GPS data, Wi-Fi signals, and other geolocation information) that reveals information about an individual’s physical movements, habits, and preferences. In particular, one of the most important requirements would be to obtain consent from the individual whose location data is being collected and used. Organizations involved in location-based advertising must include clear information in their privacy notices regarding the collection of location data, such as the type of data being collected, how the data will be used and if there will be any third-party sharing of the data.

Additionally, location-based advertising may be subject to other regulatory requirements, such as regulations from the Malaysian Communications and Multimedia Commission for mobile service providers that collect location data for advertising purposes.

7.8 How are data brokers defined and regulated under privacy law?

While data brokers are not explicitly defined under the PDPA, they are generally understood to be entities who collect, process, and sell or trade personal data, often aggregating data from multiple sources. They can be indirectly regulated by the provisions of the PDPA, as they engage in the collection, processing, and sale of personal data, often for marketing or commercial purposes. Data brokers are subject to the same obligations regarding the collection, use, and disclosure of personal data as other organizations under the PDPA (see question 4.1).

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors is regulated under the PDPA.

The consent of a minor is not typically considered valid unless the minor is of sufficient age to understand the nature of the data collection and use (generally above 13 years old). For minors below the age of 13, the consent of a parent or legal guardian is generally deemed acceptable.

Organizations should only collect personal data that is absolutely necessary for the marketing or advertising purpose in question, and should avoid the collection of data that may be deemed inappropriate for minors. Given the vulnerable nature of children's data, it is critical for advertisers to implement strict safeguards to prevent unauthorized access or misuse of minors' data.

In addition to the PDPA, there are other regulations and guidelines in Malaysia that specifically address advertising practices aimed at children or minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Privacy laws, particularly the PDPA, regulate profiling, artificial intelligence ('AI'), and automated decision-making technology used for advertising purposes by requiring consent, transparency, and ensuring the fair use of personal data.

As AI technologies evolve, regulatory frameworks may further address the complexities of automated decision-making in advertising, aiming to balance innovation with the protection of individuals' privacy rights.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Transfer of personal data to a third party or to countries outside Malaysia must be done with the prior consent of the data subject. Additionally, a data user may only transfer personal data to a place outside Malaysia under the following circumstances:

- (a) the transfer is necessary for the performance of a contract between the data subject and the data user;
- (b) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which is entered into at the request of the data subject or is in the interest of the data subject;
- (c) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- (d) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in any manner which would be a contravention of the PDPA;
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or
- (f) the transfer is necessary as being in the public interest.

There are no explicit prohibitions on transferring personal data to specific countries under the PDPA. However, if the data user transfers data to a jurisdiction that is not deemed to provide adequate data protection, the data user must implement safeguards, such as Standard Contractual Clauses ('SCC').

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Companies may need to consider other legal and regulatory obligations that could affect data transfers, such as confidentiality, legal privilege, and contractual requirements within group companies.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Malaysia? Are there minimum standards? Does this differ by sector or size of the entity?

The PDPA provides that a data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard to:

- (a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;
- (b) the place or location where the personal data is stored;
- (c) any security measures incorporated into any equipment in which the personal data is stored;
- (d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- (e) the measures taken for ensuring the secure transfer of the personal data.

9.2 How are personal data breaches regulated in Malaysia? What are the requirements for notification and response?

Personal data breaches are regulated under the PDPA, which aims to safeguard personal data processed by data users. Data users must notify both the Commissioner and affected data subjects of personal data breaches. 'Personal data breach' is broadly defined under the PDPA as any breach, loss, misuse or unauthorized access of personal data. Failure to comply may result in a fine of up to RM250,000, or imprisonment for a term of up to two years, or both.

The Personal Data Protection Guideline: Data Breach Notification requires data users to notify the Commissioner of personal data breaches where the personal data breach causes or is likely to cause 'significant harm' to the data subjects or is of a 'significant scale'. Data users must also inform the affected individuals of the personal data breach if the personal data breach results in or is likely to result in 'significant harm' to the individuals. 'Significant harm' includes instances where there is a risk that the compromised personal data may result in physical harm, financial loss, negative effects on the data subject; may be misused for illegal purposes; consists of sensitive personal data, etc. 'Significant scale', on the other hand, refers to instances where the number of affected individuals exceeds or is likely to exceed a certain numeric threshold (in this case, 1,000 individuals).

Data users must notify the Commissioner of the personal data breach as soon as practicable but no later than 72 hours after the occurrence of the data breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties have recently been made much more severe, so that businesses can now receive fines of up to RM 1 million (up from RM 300,000) and individuals within the business—such as a director, chief

executive officer, chief operating officer, manager, secretary, or other similar officer—may be held personally liable and subject to imprisonment for up to three years (up from two years) if the offence was committed with their knowledge, consent, or connivance, and was due to their failure to reasonable precautions and exercise due diligence, for breaching one of the seven principles of the PDPA (see question 4.1). The PDPA also provides for other more stringent penalties in respect of other offences.

10.2 Do consumers have a private right of action? What remedies are available to them?

Private individuals have no private rights of action specific to privacy per se, but, where the breach of privacy gives rise to damage, there may be cause of action under the general legal framework.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The PDPC has been increasingly proactive in investigating privacy breaches, issuing fines, and taking corrective actions to enforce data protection laws.

In December 2022, Telekom Malaysia (“TM”) experienced a data breach affecting 250,248 customers. The compromised data included customer names, phone numbers, and email addresses. TM promptly notified the affected customers and reported the incident to relevant authorities.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Malaysia?

None; except for religious or racial harmony.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

The following key changes have recently come into force and their effects should be closely monitored:

- (a) direct obligations on data processors to comply with the security principle,
- (b) changes to cross-border transfer rules,
- (c) revised definitions of ‘sensitive personal data’ and ‘personal data’,
- (d) increased upper limits of criminal penalties for contravening any of the personal data protection principles under the PDPA (see question 4.1);
- (e) data protection officer (‘DPO’) appointment to oversee compliance with the PDPA and serve as a point of contact for data protection matters,
- (f) mandatory data breach notifications, and
- (g) data subjects now have the right to request a data user to transmit their personal data to another data user of their choice, subject to technical feasibility and compatibility of the data format.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No identification card or passport may be retained for any period—only may be for identification purposes as necessary and should be returned promptly after use unless there is a legal or contractual requirement to retain them longer.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

In addition to the changes discussed in question 11.2, Malaysia's Cyber Security Act, which was gazetted on 26 June 2024 and came into force on 26 August 2024, introduces measures to better protect digital infrastructures, with a particular focus on data protection.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The law often struggles to keep pace with the rapid advancement of technology. This is especially true for organizations that must navigate evolving technologies—such as artificial intelligence, big data, and the Internet of Things—whilst balancing the obligations set out in existing privacy legislation. Moreover, with the increasing reliance on cloud computing and cross-border data flows, companies face increased complexities in ensuring compliance with both local and international data protection standards.

12.3 What do you envision the privacy landscape will look like in five years?

The privacy landscape in Malaysia will likely evolve significantly in the next five years, with biometric data becoming more commonplace for private use, but also being subject to stronger regulatory oversight. At the same time, more comprehensive regulation will likely be introduced for data users, processors, and brokers, ensuring better protection of personal data and greater accountability. These changes will be driven by the need for stronger privacy protection, global data protection trends, and advances in technology.

 MEXICO 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Mexico.

In Mexico, privacy is recognized as a fundamental human right under the Federal Constitution. The legal framework focuses on protecting personal data and ensuring individuals' control over their information. Privacy regulation applies primarily to private entities through the Federal Law on the Protection of Personal Data Held by Private Parties 2025 ('LFPDPPP'), which sets principles and obligations for the responsible handling of personal data. Complementary rules, such as the Regulation of the LFPDPPP and sector-specific guidelines, further refine these obligations.

1.2 What are the primary laws regulating privacy in Mexico? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary laws regulating privacy in Mexico are:

- (a) Federal Constitution: this recognizes data privacy as a human right;
- (b) LFPDPPP: this is the key regulation for private-sector entities, including those engaged in advertising and marketing activities;
- (c) Regulation of the LFPDPPP ('Regulation'): this provides detailed compliance requirements;
- (d) Consumer Protection Law: this includes provisions regarding the responsible use of personal data in advertising, specifically prohibiting unsolicited marketing (spam) without consent;
- (e) Local civil codes: for example, Mexico City's Civil Liability Law addresses violations of privacy rights; and
- (f) International agreements: Mexico is part of the Convention 108+ and the APEC Privacy Framework, which influence cross-border data handling.

Sector-specific regulations such as NOM-247-SE-2021 and standards for e-commerce platforms also impose obligations relevant to marketers, especially regarding the handling of financial and identification data in commercial transactions.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation serves as an important complement to Mexico's privacy framework. The LFPDPPP promotes the adoption of binding self-regulation schemes by companies, such as advertisers. These schemes typically include codes of conduct, best practices, or trust seals, which are validated by the relevant authority. For advertisers, self-regulation fosters consumer confidence and signifies a dedication to data management practices that exceed legal requirements.

1.4 How is privacy law enforced in Mexico? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The LFPDPPP is enforced by the Secretariat for Anti-Corruption and Good Governance ('Secretariat') replacing the previous enforcement body, INAI, which can impose penalties for non-compliance. See questions 10.1 and 10.2. Exceptions are made for non-commercial data processing and credit reporting agencies governed by separate regulations.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Mexico?

In Mexico, the LFPDPPP and its Regulation applies to all private entities that handle personal data for commercial, professional, or business purposes—both individuals and organizations—that manage (process) personal data as part of their business operations. This includes marketing agencies, advertisers, and digital platforms that collect, use, or store personal information. The law applies regardless of the size or industry of the company, except for specific exemptions such as credit information agencies (regulated under separate legislation) or individuals processing data solely for personal use without commercial intent.

2.2 Does privacy law in Mexico apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Mexico's data privacy laws apply to foreign companies under specific conditions, particularly when they operate within the country's jurisdiction or process data related to Mexican residents. The LFPDPPP governs these obligations, requiring compliance from foreign entities with a physical presence in Mexico (eg, subsidiaries or branches) or those engaging in data processing activities targeting Mexican users. However, companies operating entirely outside Mexico are generally exempt unless bound by contractual obligations or international treaties.

Foreign companies must fulfill key requirements, including issuing privacy notices that disclose data collection purposes, enabling individuals to exercise their ARCO rights (ie rights of Access, Rectification, Cancellation, and Opposition), and ensuring secure handling of personal data. Data transfers to third parties abroad must also comply with local regulations, requiring recipients to adhere to equivalent privacy standards. Notably, local representation is not mandatory, but businesses must provide accessible channels for data subjects to exercise their rights.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Mexico?

Personal data refers to any information concerning an identified or identifiable individual. An individual is considered identifiable when their identity can be determined directly or indirectly through any piece of information.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Sensitive data includes racial origin, health status, genetic info, religious beliefs, political opinions, and sexual preferences. Processing requires explicit consent.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Mexican privacy law recognizes the concept of disassociation (similar to anonymization). When personal data is disassociated, meaning it cannot be linked back to an individual, it is no longer considered subject to the same legal obligations as identifiable personal data. However, companies must ensure that the disassociation process is robust and irreversible.

Pseudonymized data, where identifiers are removed but can be re-linked, is still considered personal data and must comply with all legal requirements, including consent, security, and privacy notice obligations.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Mexican Privacy Law imposes several key obligations on companies, particularly relevant for marketing and advertising activities:

- (a) Companies must provide clear, accessible privacy notices detailing how personal data is collected, used, and shared;
- (b) Companies must enable individuals to exercise their rights of Access, Rectification, Cancellation, and Opposition ('ARCO') regarding their personal data;
- (c) Data collected should be limited to what is necessary for the intended purpose;
- (d) Companies must obtain appropriate consent before processing data, particularly for financial, sensitive and/or marketing purposes;
- (e) Agreements with vendors or service providers must include clauses ensuring compliance with privacy obligations;
- (f) Administrative, technical, and physical safeguards must be in place to protect personal data; and
- (g) Staff involved in data handling should be trained on privacy practices and legal requirements.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Under the LFPDPPP, companies are assigned roles based on their processing activities, specifically as 'responsible' parties (controllers) or 'persons in charge' (processors). These roles significantly affect their obligations:

- (a) **The responsible party (controller)** decides the purposes and means of processing personal data. Their obligations include providing a privacy notice, obtaining consent, ensuring data minimization, implementing security measures, maintaining accurate records, training employees, and ensuring confidentiality.
- (b) **The person in charge (processor)** processes personal data on behalf of the controller. Their obligations include complying with the controller's instructions, implementing security measures, maintaining confidentiality, and assisting the controller in fulfilling their legal obligations.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The LFPDPPP requires a lawful basis for processing personal data, primarily through the consent of the data subject. Consent must be free, specific, informed, and explicit, especially for sensitive personal data, which requires written consent. However, there are exceptions where consent is not required, such as legal obligations, publicly accessible sources, disassociation procedures, contractual relationships, emergency situations, medical necessity, and judicial or administrative orders.

Additionally, data processing must adhere to principles of lawfulness, purpose specification, proportionality, and quality to protect the privacy and rights of data subjects.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

- (a) **Identity and address of the data controller:** the company must clearly indicate the identity and physical address of the entity responsible for processing the personal data;
- (b) **Personal data being processed:** the company must specify the categories of personal data collected, including any sensitive personal data, if applicable;
- (c) **Purposes of data processing:** the company must detail the purposes for which the personal data will be processed. It is essential to distinguish between purposes that require the data subject's consent (such as advertising and marketing communications) and those that do not;
- (d) **Options and means to limit use or disclosure:** the company must provide information on the available options and mechanisms for data subjects to limit the use or disclosure of their personal data, such as opt-out options for receiving marketing communications;
- (e) **Mechanisms for exercising ARCO rights:** the company must include the procedures, means, and contact details for data subjects to exercise their ARCO rights—Access, Rectification, Cancellation, and Opposition (Objection); and
- (f) **Changes to the privacy notice:** the company must explain the process and means by which data subjects will be informed of any modifications to the privacy notice.

For advertising and marketing purposes specifically, the most relevant elements are the purposes of data processing—particularly emphasizing that the processing of personal data for advertising requires the explicit consent of the data subject, and the options and means to limit use or disclosure, allowing individuals to opt out of receiving promotional content.

When data is obtained through electronic or technological means, at minimum, a simplified version of the notice must be provided, containing key information such as the identity of the data controller, purposes of processing, and mechanisms to limit data use, while indicating where the full notice can be consulted.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

- (a) **Cancellation:** The right to request deletion of personal data when it is no longer needed.
- (b) **Opposition:** The right to object to the use of personal data, particularly for marketing purposes.
- (c) **Revocation of consent:** Data subjects can withdraw their consent for the processing of their personal data. It is important to note that revocation is not retroactive, meaning it does not affect data processing that occurred prior to the withdrawal.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies are required to obtain the data subject's consent when processing personal data for every kind of purpose, including advertising. Consent may be express—through any clear affirmative action—or tacit, meaning the individual is informed via the privacy notice and does not object.

Additionally, companies must provide data subjects with clear opt-out options to limit the use or disclosure of their personal data for marketing purposes, allowing individuals to restrict how their data is used. Typical examples include unsubscribe links in marketing emails or customer service channels for managing consent preferences.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Mexican privacy law requires that when companies engage vendors—such as advertising agencies, demand-side platforms (DSPs), or data providers—to process personal data on their behalf, they must:

- (a) Ensure that contracts clearly define the roles and responsibilities of both the company (controller) and the vendor (processor);
- (b) Require vendors to process data only according to the company's instructions and not use it for unauthorized purposes;
- (c) Mandate that vendors implement security measures to protect personal data; and
- (d) Ensure vendors respect the same confidentiality and compliance obligations as the company itself.

This is essential to mitigate risks related to third-party misuse of personal data in advertising ecosystems.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When disclosing or receiving personal data to third parties, companies must enter into contracts containing:

- (a) Explicit clauses on data processing purposes, limiting data use to what is agreed;
- (b) Provisions ensuring compliance with the LFPDPPP and applicable regulations;
- (c) Obligations for vendors to adopt administrative, technical, and physical safeguards;
- (d) Requirements for vendors to maintain confidentiality and delete personal data once services end; and
- (e) Prohibitions on data transfers to unauthorized parties unless instructed by the company or legally required.

These contracts serve as critical compliance tools, particularly in advertising partnerships where data flows between multiple parties.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must implement appropriate safeguards when engaging vendors and partners for advertising activities, including:

- (a) Requiring vendors to maintain confidentiality and use personal data only for specified advertising purposes;
- (b) Ensuring vendors apply adequate technical, administrative, and physical security measures; and
- (c) Verifying that vendors comply with privacy principles and assist in fulfilling data subjects' rights, such as access or opt-out requests.

Although Mexican law does not require explicit notification of each vendor transfer, companies remain accountable for ensuring third parties uphold the same data protection standards. Establishing clear contractual obligations and oversight mechanisms helps demonstrate compliance and maintain consumer trust.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing activities—such as emails, text messages, or push notifications—are regulated under Mexican privacy law by requiring companies to:

- (a) Obtain valid consent before using personal data for marketing purposes.
- (b) Clearly inform individuals in the privacy notice about how their data will be used for direct marketing.
- (c) Provide accessible opt-out mechanisms, allowing individuals to withdraw consent or stop receiving promotional communications at any time.

Additionally, companies must ensure that all marketing communications comply with general privacy principles, including purpose limitation, proportionality, and data security. Maintaining records of consent and opt-out requests is also considered best practice to demonstrate compliance and accountability.

Finally, unsolicited communications (spam) are prohibited under the LFPDPPP.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies such as cookies, pixels, and SDKs are regulated under Mexican privacy law through transparency and consent requirements. Companies must:

- (a) Inform individuals, typically via a clear and accessible cookies or tracking notice, about the use of these technologies and the types of data collected;
- (b) Specify the purposes of tracking, especially when used for advertising, analytics, or profiling; and
- (c) Obtain consent when tracking involves personal data and is not strictly necessary for service delivery.

Although the law does not prescribe detailed technical rules for cookies or SDKs, applying consent banners and offering users control over non-essential tracking is recognized as a best practice to align with privacy principles and reduce compliance risks.

7.3 How are loyalty programs and promotions regulated under privacy law?

While there is no specific law governing loyalty programs, companies must:

- (a) Clearly disclose how participants' personal data will be used;
- (b) Obtain consent when collecting data for purposes beyond program administration (eg, cross-selling, profiling); and
- (c) Allow participants to exercise their ARCO rights regarding their data.

Additionally, the Consumer Protection Law imposes transparency requirements on promotions to ensure fairness.

7.4 How is social media and influencer marketing regulated under privacy law?

- (a) Whilst there are no specific privacy legislation governing social media and influencers, companies should ensure any personal data shared during campaigns complies with standard protocols. The general privacy regulations apply equally to personal data collected via social media platforms. Companies must:

- (i) Ensure data collected from social media is processed in compliance with privacy notices and consent mechanisms; and
- (ii) Recognize that whilst social media profiles may constitute public access sources, this does not override obligations to inform and respect user rights.

It is also relevant to mention that the Federal Consumer Protection Law is the main legislation regulating commercial advertising.

- (b) The Mexican Consumer Protection Agency has published the Influencers Guide, which is a non-binding document that includes the following recommendations for content creators:
 - (i) Always place the information in a visible and available place;
 - (ii) Do not use or post information accompanied by various labels or links that make it difficult, confusing or impede that it is advertising;
 - (iii) In the case of images or videos, include the reference to the advertisement in such a way that it can be read and appreciated throughout its duration;
 - (iv) Use labels that are easy to understand. In the case of audio media, expressly mention that it is advertising;
 - (v) Check the websites of goods, products or services to ensure that they are safe and compliant. If possible, share the source so consumers can verify the information; and
 - (vi) Ensure that the opinion expressed by the influencer or content creator is limited to the experience with the good, product or service. It is valid to express an opinion when the experience was not good.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

According to Mexican Law, there is no distinction between targeted, behavioral, or contextual advertising concerning privacy regulations. Companies must adhere to standardized protocols ensuring compliance with privacy notices and consent mechanisms for all forms of advertising. This means that irrespective of whether the advertising is personalized or based on page content, companies are required to:

- (a) Clearly inform individuals of data collection and profiling activities;
- (b) Obtain valid consent before processing personal data for profiling or delivering personalized ads;

- (c) Clearly inform individuals in the privacy notice about the use of their data for targeted advertising and offer easy opt-out options;
- (d) Provide opt-out options for personalized ads; and
- (e) Ensure vendors and partners handling personal data for these purposes follow the same privacy obligations.

Mexican Law mandates uniform privacy practices across all advertising types, emphasizing the importance of safeguarding user rights and maintaining transparency in data processing activities.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

While there is no explicit mention of these technologies in Mexican law, they are subject to general privacy principles:

- (a) Companies must inform individuals how their data is combined or matched across platforms (identity resolution); and
- (b) For clean rooms, any sharing of personal data with partners must comply with consent, security, and contractual obligations.

7.7 How is location-based advertising regulated under privacy law?

Location data is considered personal data, and often sensitive if it reveals habits or frequent locations. Companies must:

- (a) Obtain explicit consent for collecting and using precise location data;
- (b) Inform users about how location data will be used, especially if shared with advertisers or partners; and
- (c) Provide opt-out options.

7.8 How are data brokers defined and regulated under privacy law?

Under the Mexican legal framework, the figure of a data broker, specifically involved in the selling of personal data, does not formally exist. This is because the commercialization of personal data is not permitted. Nevertheless, any entity that collects, processes, or transfers personal data must adhere to the general obligations set forth by the LFPDPPP.

7.9 How is advertising to children and minors regulated under privacy law?

Mexico recognizes children's data as particularly sensitive. Thus, companies must also ensure that their advertising content does not exploit the vulnerabilities of children or minors. This includes avoiding deceptive practices that may mislead young audiences or manipulate their understanding of the product or service being advertised.

Additionally, general advertising laws impose restrictions on marketing content directed at children.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

While Mexican law does not have specific provisions exclusively for AI or profiling in advertising, general data protection principles—such as purpose limitation, proportionality, and safeguarding individuals' rights—apply. Conducting risk assessments and ensuring human oversight over automated processes are considered best practice to enhance compliance and accountability.

7.11 Are there other specific advertising practices that you wish to discuss?

While not explicitly regulated, companies engaging in programmatic advertising, data matching, or cross-device tracking should ensure all data handling complies with the privacy principles. Adopting voluntary self-regulatory frameworks can also strengthen consumer trust and demonstrate compliance efforts.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes, national and international transfers of personal data are regulated under Mexican privacy law:

- (a) **Consent requirement:** Personal data can only be transferred to third parties, including entities in other jurisdictions, if the individual has given prior consent, except in certain legal exceptions (eg, intra-group transfers, legal obligations).
- (b) **Privacy notice obligation:** The transferring company must inform the third party of the purposes and limitations agreed upon by the data subject.
- (c) **Minimum safeguards:** The third party receiving the data must comply with the same privacy and security standards as the data controller in Mexico.

There are no explicit restrictions on specific countries, but companies must ensure adequate protection levels in the destination jurisdiction, even though Mexico does not operate a formal ‘adequacy list.’

Standard contractual clauses are not mandatory by law but are considered best practice to ensure compliance and mitigate risks.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Yes, additional considerations include:

- (a) Personal data can only be transferred to third parties, including entities in other jurisdictions, if the individual has given prior consent, except in certain legal exceptions such as:
 - (i) inter-company transfers within the same corporate group,
 - (ii) when the transfer is required by law or an international treaty to which Mexico is a party,
 - (iii) when the transfer is necessary for medical diagnosis or treatment, or
 - (iv) when the transfer is essential to safeguard public interest or for the administration of justice;
- (b) The transferring company must inform the third party of the purposes and limitations agreed upon by the data subject;
- (c) Data transfers involving sensitive personal data require explicit consent and must meet higher security standards;
- (d) Companies should maintain documentation of data transfers for accountability and audit purposes; and
- (e) In the absence of formal ‘privilege’ rules in data transfers, companies must avoid sharing data that could breach contractual confidentiality or regulatory obligations.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Mexico? Are there minimum standards? Does this differ by sector or size of the entity?

In Mexico, data security is a mandatory obligation under the LFPDPPP. Companies must implement administrative, technical, and physical security measures to protect personal data from unauthorized access, loss, alteration, or misuse.

Key points:

- (a) While the law does not prescribe specific technologies, it requires measures to be proportional to the sensitivity of the data, the potential risks, and the size and capabilities of the company;
- (b) INAI has published best practices (non-binding but highly recommended) for developing a Data Security Management System (although the INAI has been formally dissolved, these recommendations remain valid and relevant); and
- (c) For certain industries (eg, financial, healthcare, fintech), additional security obligations may apply through sectoral regulations (such as NOM-247-SE-2021 for housing and fintech regulations).

Smaller entities are required to comply with security measures that are suitable for their available resources but must still maintain some level of security.

9.2 How are personal data breaches regulated in Mexico? What are the requirements for notification and response?

Mexican privacy law requires:

- (a) Immediate notification to affected individuals if a data breach significantly affects their moral or economic rights.
- (b) The notification must include:
 - (i) The nature of the breach;
 - (ii) The compromised personal data;
 - (iii) Recommendations to protect the data subject's interests;
 - (iv) Corrective actions taken by the company; and
 - (v) Contact details for further information.

Although there is no formal timeline (eg, 'within 72 hours'), the law specifies that notification should be without undue delay.

Additionally, companies must internally document the breach and may be subject to verification by the Secretariat.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The LFPDPPP establishes a comprehensive penalty framework for privacy law non-compliance, with warnings and fines ranging from 100 to 320,000 times the UMA, potentially doubling for sensitive data. With the UMA at 113.14 pesos daily as of February 2025, fines can reach into the tens of millions,

emphasizing the need for stringent compliance. Marketing teams must integrate these risks into their strategies, considering both financial and legal ramifications.

The Secretariat is responsible for investigating violations and imposing administrative sanctions.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under the LFPDPPP, consumers do not have a direct right to sue for privacy violations. Instead, enforcement is primarily handled through administrative actions by the Secretariat, which can impose fines and sanctions. Consumers can exercise ARCO rights and file complaints if their requests are not addressed in a timely manner, leading to regulatory actions.

The law also doubles penalties for violations involving sensitive data, increasing financial risks for companies.

For marketing professionals, this highlights the importance of complying with ARCO rights and data protection regulations, to avoid significant fines and ensure consumer trust.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Given the current transitional phase between authorities (from INAI to the Secretariat), there is insufficient information to accurately project a trend in the performance of this authority. Nevertheless, based on the general behavior of other authorities since the change of administration, it is anticipated that there will be an increase in enforcement in this area.

That said, INAI had itself become increasingly active in the years before its dissolution, conducting audits, verifications, and sanctions, particularly targeting sectors like financial services, e-commerce, and telecommunications.

In the advertising context, enforcement has focused on:

- (a) Unauthorized direct marketing campaigns without proper consent.
- (b) Lack of clear privacy notices or failure to offer opt-out mechanisms.
- (c) Improper handling or sharing of customer databases with third parties without informing users.

For example, the INAI sanctioned companies for sending unsolicited promotional emails and failing to allow consumers to exercise their ARCO rights effectively.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Mexico?

Yes. In Mexico, privacy is deeply connected to constitutional human rights, fostering a strong cultural expectation of informational self-determination. Historically, enforcement was centralized through the National Institute for Transparency, Access to Information, and Personal Data Protection (INAI). However, following a recent constitutional reform on administrative simplification, the INAI has been dissolved, and a new authority, the Secretariat for Anti-Corruption and Good Governance is now tasked with privacy oversight, transparency, and access to information. This shift reflects a broader cultural emphasis on government efficiency, accountability, and integrity, influencing how enforcement and regulatory approaches are applied.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) **LFPDPPP:** The updated law introduces structural, definitional, and procedural changes, including:
 - (i) Replacement of INAI by the Secretariat for Anti-Corruption and Good Governance as the primary authority,
 - (ii) Expanded definitions, such as clearer criteria for identifiable persons and enhanced definitions of sensitive data, consent, and data processing,
 - (iii) More explicit guidance on privacy notices, especially regarding digital environments and specific consent requirements,
 - (iv) Stronger emphasis on data subject rights (ARCO rights) and detailed procedures for exercising them,
 - (v) Updates on data transfers, requiring clearer clauses in privacy notices and reinforced obligations on third-party recipients, and
 - (vi) Reinforced provisions for self-regulation mechanisms, requiring them to be notified to the Secretariat;
- (b) **Focus on cybersecurity and digital platforms:** The law now emphasizes information security, including risk-based measures aligned with technological advancements.
- (c) **Potential challenges:** Transitioning compliance frameworks from INAI to the new Secretariat authority may require internal policy updates and contractual revisions.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Companies in marketing and advertising should:

- (a) Anticipate stricter scrutiny on consent mechanisms, particularly for digital advertising and cross-border campaigns;
- (b) Update privacy policies and contracts to reflect the shift in authority and the expanded definitions from the 2025 reform; and
- (c) Consider participating in binding self-regulation schemes, which remain encouraged as a best practice and are now overseen by the new Secretariat.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, the most significant change has been the elimination of the INAI and the transfer of responsibilities to the Secretariat for Anti-Corruption and Good Governance. This was triggered by a constitutional reform aimed at reducing administrative complexity and enhancing anti-corruption efforts.

The repeal of the 2010 Data Protection Law and its replacement by the 2025 LFPDPPP, along with the ongoing updates to related regulations, represent a major shift in Mexico’s data privacy landscape.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

- (a) Adapting internal processes and compliance programs to reflect the new regulatory authority and legal definitions;
- (b) Ensuring marketing strategies comply with more detailed consent and transparency requirements;
- (c) Reviewing and updating contracts, privacy notices, and ARCO request procedures; and
- (d) Preparing for potential audits and verifications under a different enforcement body.

12.3 What do you envision the privacy landscape will look like in five years?

Over the next five years, Mexico's privacy framework will likely evolve to:

- (a) see increased inter-agency collaboration on cybersecurity and digital identity;
- (b) emphasize automated decision-making, AI profiling, and children's online privacy, areas highlighted but not yet heavily regulated; and
- (c) encourage greater industry participation in self-regulation and certification programs, fostering consumer trust in the digital economy.

MOROCCO

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Morocco.

Privacy in Morocco is regulated primarily under Law No 09-08 on the Protection of Individuals with Regard to Processing of Personal Data ('Personal Data Protection Law'), enacted in 2009. The law establishes the legal framework for data processing activities and is complemented by various decrees and resolutions issued by the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ('CNDP'), the national data protection authority. Morocco has also ratified Convention 108+ to align with international data protection standards.

1.2 What are the primary laws regulating privacy in Morocco? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy law in Morocco is governed by:

- (a) Personal Data Protection Law—this defines data protection principles, obligations, and rights;
- (b) Decree No 2-09-165—this implements the Data Protection Law; and
- (c) Convention 108+—this is an international treaty on data protection ratified by Morocco.

Other relevant Laws:

- (d) Moroccan Constitution (2011)—this guarantees privacy rights;
- (e) Cybersecurity Law No 05-20—which addresses digital security;
- (f) Consumer Protection Law No 31-08—which regulates commercial data processing; and
- (g) Right of Access to Information Law No 31-13—which ensures transparency in public data handling.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

While Moroccan law does not mandate self-regulation, the CNDP issues sector-specific guidelines that companies are expected to follow, particularly for digital marketing and facial recognition technologies. The authority has also introduced compliance frameworks for banks, social security institutions, and political entities.

1.4 How is privacy law enforced in Morocco? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The CNDP is the principal enforcement body, responsible for:

- (a) reviewing and approving data processing declarations and authorizations;
- (b) conducting investigations and audits;
- (c) issuing fines and sanctions for non-compliance; and
- (d) overseeing international data transfers.

Violations can result in fines up to MAD 200,000 (approx USD 22,500) and imprisonment for severe breaches.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Morocco?

The law applies to all entities processing personal data in Morocco, including:

- (a) businesses and public authorities collecting or processing personal data; and
- (b) foreign companies using infrastructure in Morocco for data processing.

2.2 Does privacy law in Morocco apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. Foreign companies processing the data of Moroccan residents must comply with local privacy regulations, and may be required to appoint a local representative if they process personal data within Moroccan territory.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Morocco?

'Personal data' includes any information identifying a natural person, such as names, ID numbers, biometric data, and digital identifiers.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

'Sensitive data' includes information about racial or ethnic origin, religious beliefs, political opinions, health, genetics, and criminal records. Processing sensitive data requires explicit consent or legal authorization.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

While not explicitly addressed in the law, if data can be re-identified, it is subject to the Personal Data Protection Law.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must:

- (a) obtain explicit consent before collecting personal data;
- (b) ensure data minimization, purpose limitation, and security;
- (c) notify the CNDP before processing certain categories of data; and
- (d) obtain prior approval for international data transfers.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes. Companies are classified as Data Controllers or Data Processors, each with different compliance obligations.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes. Processing must be based on:

- (a) consent from the data subject;
- (b) legal obligations;
- (c) contractual necessity; and
- (d) legitimate interests, subject to CNDP approval.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The following information should be included:

- (a) purpose of data collection;
- (b) legal basis for processing;
- (c) retention period; and
- (d) consumer rights and redress mechanisms.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the following rights:

- (a) right to access, correct, and delete their personal data;
- (b) right to withdraw consent; and
- (c) right to object to processing, especially for marketing.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Opt-in consent is required for direct marketing via email, SMS, or automated calls.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Controllers must verify that vendors have appropriate security and compliance frameworks in place. The CNDP expects formal contracts to govern such processing relationships.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Third-party agreements must address data handling procedures, confidentiality, permitted use, cross-border transfer rules, and audit rights.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Controllers should vet third-party service providers through risk assessments and conduct data protection impact assessments for high-risk advertising activities, such as behavioral targeting or facial recognition.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing requires prior opt-in consent from individuals before sending communications via email, text, or push notifications. Companies must provide a clear and simple opt-out mechanism, and all communications must identify the sender and include a means for recipients to withdraw their consent.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies, such as cookies and SDKs, requires informed consent from users. Companies must provide clear disclosures about the purpose of data collection and allow users to opt out or manage their cookie preferences.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs must comply with the principles of data minimization and purpose limitation. Users must be informed about how their data will be collected and processed, and data must not be used for marketing purposes without explicit consent.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing campaigns must be transparent regarding data collection and processing practices. Users must be informed if their data is being used for profiling or advertising targeting.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising using personal data requires explicit consent from users. Contextual advertising, which does not involve personal data collection, is generally subject to fewer restrictions.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific laws addressing digital identity resolution or clean room technologies in Morocco. However, general data protection principles apply, including transparency, security, and user rights to access and rectify their data.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising requires explicit user consent before collecting geolocation data. Companies must clearly state how location data will be used and provide users with an option to disable tracking.

7.8 How are data brokers defined and regulated under privacy law?

Moroccan privacy law does not explicitly define data brokers, but entities collecting and selling personal data must comply with data protection regulations, including obtaining user consent and ensuring data security.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to minors is subject to strict regulations. Companies must obtain parental consent before processing a child's personal data and must avoid behavioral profiling of minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Automated decision-making and profiling for advertising must comply with transparency principles. Users must be informed if AI-driven advertising affects them, and have the right to contest automated decisions.

7.11 Are there other specific advertising practices that you wish to discuss?

Businesses should be aware of evolving regulatory requirements related to AI, biometric advertising, and consumer tracking in Morocco.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Cross-border data transfers are subject to prior authorization from the CNDP. Transfers to countries that do not provide adequate data protection may be restricted unless appropriate safeguards, such as standard contractual clauses, are implemented.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Organizations handling sensitive or privileged data must implement additional security measures, such as encryption. Transfers of financial, healthcare, or government-related data may be subject to sector-specific restrictions.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Morocco? Are there minimum standards? Does this differ by sector or size of the entity?

Data controllers must implement appropriate security measures to protect personal data from unauthorized access, loss, or breaches. Minimum security standards vary by sector, with financial and healthcare industries subject to stricter requirements.

9.2 How are personal data breaches regulated in Morocco? What are the requirements for notification and response?

Moroccan law does not mandate breach notifications, but the CNDP encourages voluntary reporting. Organizations must take immediate action to mitigate damage and strengthen security measures after a breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Non-compliance can result in fines ranging from MAD 10,000 to MAD 200,000. Serious violations, such as unauthorized data transfers, can lead to criminal penalties, including imprisonment.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers do not have a direct right to sue for privacy violations but may file complaints with the CNDP, which can investigate and take enforcement actions.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The CNDP actively monitors compliance, and has issued sanctions against organizations violating data protection laws. Recent cases include actions against companies engaging in unauthorized data transfers and unapproved marketing practices.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Morocco?

Privacy law enforcement in Morocco is influenced by national security interests and government oversight, which impact the application of data protection rules.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Businesses should monitor potential amendments to align Moroccan law with GDPR standards, particularly regarding AI regulation and cross-border data transfers.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Companies should establish strong compliance frameworks and regularly assess their data protection policies to remain aligned with evolving regulations.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Morocco's ratification of Convention 108+ has led to increased regulatory scrutiny of cross-border data transfers and AI-based processing.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Key challenges include obtaining regulatory approvals for international data transfers, ensuring compliance with AI-driven advertising, and adapting to increased enforcement measures.

12.3 What do you envision the privacy landscape will look like in five years?

Moroccan privacy laws are expected to align more closely with GDPR, introducing stricter data protection standards, mandatory breach notifications, and enhanced consumer rights protections.

NEW ZEALAND

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in New Zealand.

Privacy in New Zealand is regulated by a combination of statute, associated regulations and codes. There is also a common law tort of invasion of privacy. The main statute regulating privacy is the Privacy Act 2020 ('Privacy Act'). Self-regulatory frameworks, such as the Advertising Standards Authority's codes, also regulate privacy to a certain degree.

1.2 What are the primary laws regulating privacy in New Zealand? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary law regulating privacy is the Privacy Act. The Privacy Act sets out information privacy principles which are the primary principles that agencies need to follow, as further detailed at question 4.1. Under the Privacy Act, the Privacy Commissioner has the power to issue codes of practice. These codes become part of the law. The current codes of practice include:

- (a) Civil Defense National Emergencies (Information Sharing) Code 2020;
- (b) Credit Reporting Privacy Code 2020;
- (c) Health Information Privacy Code 2020;
- (d) Justice Sector Unique Identifier Code 2020;
- (e) Superannuation Schemes Unique Identifier 2020; and
- (f) Telecommunications Information Privacy Code 2020.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There are self-regulatory frameworks which regulate privacy, these include the New Zealand Advertising Standards Authority ('ASA') and its advertising codes.

1.4 How is privacy law enforced in New Zealand? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The provisions of the Privacy Act and associated codes are enforced by the Privacy Commissioner. Complaints may be made to the Privacy Commissioner if an agency's actions interfere with the privacy of an individual. Any person may make a complaint to the Privacy Commissioner. The Privacy Commissioner may then decide to investigate the complaint, refer the complaint to another authority (eg, the Human Rights Review Tribunal), or not investigate the complaint. An aggrieved individual (or their representative) may appeal a decision of the Privacy Commissioner to the Human Rights Review Tribunal, which is an independent judicial body, separate from the office of the Privacy Commissioner. Proceedings can also be brought by a representative of a class of aggrieved individuals, not just one individual.

A breach of the privacy provisions contained in the ASA's codes is enforced by the ASA. Members of the public may complain to the ASA if they believe advertising has breached one of the ASA's codes.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in New Zealand?

The Privacy Act expanded the scope of who is subject to privacy legislation in New Zealand. The Privacy Act applies to three main groups, namely:

- (a) New Zealand agencies (which include individuals ordinarily resident in New Zealand and New Zealand companies) in relation to any action taken by them in respect of personal information collected or held by them;
- (b) Overseas agencies (broadly any overseas person, body corporate or unincorporated body that is not a New Zealand agency (certain other exceptions also apply)) in relation to any action taken by them in the course of carrying on business in New Zealand in respect of personal information collected or held by them; and
- (c) Individuals who are not ordinarily resident in New Zealand in relation to any action taken by them in respect of personal information collected by them while present in New Zealand and personal information held by them while present in New Zealand.

2.2 Does privacy law in New Zealand apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the Privacy Act can apply to an overseas agency where an action is taken in respect of personal information in the course of carrying on business in New Zealand. Individuals who do not normally reside in New Zealand may also come within the provisions of the Privacy Act. See question 2.1.

The Privacy Act sets out certain restrictions on personal information being disclosed to a foreign person or entity. Disclosure is permitted in certain circumstances, including if the entity disclosing the information reasonably believes the foreign entity is subject to the Privacy Act or comparable privacy laws or has contractually agreed to protect the information in a way that is comparable to the safeguards in the Privacy Act. If this is not the case, the individual may authorize their information to be disclosed, but only once they have been informed that the foreign entity may not be required to protect their information in the same or a comparable way to the Privacy Act.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in New Zealand?

The Privacy Act defines 'personal information' as information about an identifiable individual, and includes information relating to a death.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

- (a) The Privacy Act does not specifically define 'sensitive personal information'; the definition of 'personal information' means that the Privacy Act applies to all personal information, not just or specifically sensitive information. The Privacy Act does, in some instances, specify how certain information must be treated. For example, Principle 4, which generally requires personal information to be collected only by a lawful means and by a means that in the circumstances is fair and does not intrude to an unreasonable extent into the personal affairs of the individual, specifically highlights that such requirements are particularly important where the personal information is collected from young children/people.

- (b) The codes of practice issued by the Privacy Commissioner (see question 1.2) are also examples of areas where there are specific privacy requirements. Examples include:
 - (i) the Health Information Privacy Code which sets out rules for the health sector, and
 - (ii) the Credit Reporting Privacy Code which sets out specific rules for credit reporters.
 The Privacy Commissioner intends to issue a Biometric Processing Privacy Code of Practice in 2025.
- (c) The ASA also recognizes the sensitivity of personal information relating to children in its Children’s Advertising Code. See question 7.9.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Agencies generally cannot disclose personal information unless one of the permitted grounds for disclosure set out in the Privacy Act applies. Permitted grounds include where the agency disclosing the information believes on reasonable grounds that the information is in a form which does not risk revealing personal details about an identifiable person.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) The Privacy Act sets out 13 Information Privacy Principles which are the key principles that agencies need to follow. A summary of the principles is set out below.
 - (i) **Principles 1–4: Collection:** Personal information can only be collected for lawful purposes, and its collection must be necessary for that purpose. If the lawful purpose does not require collection of identifying information, the agency may not require that the identifying information be provided. The information should be collected directly from the individual, unless certain circumstances apply, for example if the individual authorizes the collection of the information from someone else.
 When the information is collected, the individual needs to be made aware that:
 - the information is being collected;
 - the purpose for which the information is being collected;
 - the intended recipients of the information;
 - the name and address of the entity that is collecting the information and the entity that will hold the information;
 - if the information is authorized or required by law, details of this;
 - the consequences (if any) if all or any part of the information is not provided; and
 - the person’s right to access, and correct personal information.
 Personal information cannot be collected by unlawful means or by means that, in the circumstances are unfair or intrude to an unreasonable extent on the personal affairs of the individual.
 - (ii) **Principle 5—Storage and security of personal information:** Personal information must be protected, by such safeguards as are reasonable in the circumstances, against loss, access, use, modification or disclosure not authorized by the agency and other misuse.

- (iii) **Principles 6–8—Access to, correction and accuracy of personal information:** Individuals have the right to access and correct personal information. This is subject to certain limitations, such as where the disclosure would endanger the safety of an individual, or if the information cannot easily be retrieved. An agency holding personal information should not use that information without taking any steps that are reasonable in the circumstances, to ensure that the information is accurate, up to date, complete, relevant and not misleading.
 - (iv) **Principle 9—Retention:** Personal information should only be held for the time period required for the purpose for which it may be lawfully used.
 - (v) **Principle 10—Use:** Personal information may only be used for the purpose for which the individual was advised it was collected. There are a very limited number of exceptions to this, for example if the information is used in a form in which the individual is not identified.
 - (vi) **Principle 11—Disclosure:** Personal information may only be disclosed if that disclosure is one of the purposes in connection with which the information was obtained or is directly related to the purposes for which the information was obtained. Disclosure that is authorized by the individual concerned or to the individual concerned is also permitted. There are also a limited number of further permitted disclosures, such as if the disclosure is necessary to prevent a serious threat public safety.
 - (vii) **Principle 12—Disclosure to foreign persons or entities:** There are also conditions which must be met for an agency to disclose personal information under Principle 11 to a foreign person or entity. For example, the agency must believe (on reasonable grounds) that the foreign person/entity is subject to the Privacy Act (if trading in New Zealand) or privacy laws with comparable safeguards.
 - (viii) **Principle 13—Unique identifiers:** An agency cannot require an individual to disclose any unique identifier (which would include for example a passport number) unless disclosure is for one of the purposes for which that unique identifier was assigned or for a purpose that is directly related to one of those purposes. An agency may only assign a unique identifier to an individual if it is necessary to carry out one or more of its functions efficiently.
- (b) In addition to compliance with the information privacy principles, the Privacy Act requires that each agency has at least one privacy officer. the responsibilities of a privacy officer include:
- (i) encouraging compliance with the information privacy principles,
 - (ii) dealing with any requests made under the Privacy Act,
 - (iii) working with the Privacy Commissioner in relation to any investigations, and
 - (iv) otherwise ensuring compliance by the organization with the Privacy Act.
- (c) If a notifiable privacy breach occurs, the agency must follow the notification requirements set out in the Privacy Act. This is further detailed at question 9.2.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

No, the Privacy Act does not assign different roles to companies based on their processing activities.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

As detailed at question 4.1, personal information can only be collected for lawful purposes, and its collection must be necessary for that purpose. Personal information may only be used (or processed) for the purpose for which the individual was advised it was collected. There are very limited exceptions to this.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Personal information must generally be collected from the individual concerned, and that individual must be made aware, generally through a privacy notice, of the following:

- (a) that the information is being collected;
- (b) the purpose for which the information is being collected;
- (c) the intended recipients of the information;
- (d) the name and address of the agency that is collecting the information and the entity that will hold the information;
- (e) if the information is authorized or required by law, details of this;
- (f) the consequences (if any) if all or any part of the information is not provided; and
- (g) the person's right to access, and correct personal information.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Pursuant to the Privacy Act, individuals generally need to be informed when their personal information is being collected and what it will be used for. Accordingly, if information is being collected for the purposes of being used in an advertisement the individual should generally be made aware of this.

In addition to the information privacy principles under the Privacy Act, there are additional guidelines in the ASA's Advertising Standards Code. For example, advertisements should only portray or refer to personal information that is publicly available. Other personal information may only be collected and used with the consent of the individual concerned.

The ASA has published the following guidelines in relation to the interpretation of this rule:

- (a) 'Personal information that is publicly available' means information about an identifiable individual that is available to the public eg, contained in a publicly available publication;
- (b) Publicly available information must not be disclosed if doing so would be unfair or unreasonable in the circumstances;
- (c) When personal information (including images) is collected, it must be clear to the individual how their information will be used in an advertisement; and
- (d) Consent of a parent or guardian must be obtained before personal information (including images) of anyone under the age of 18 is used in an advertisement.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

The Unsolicited Electronic Messages Act 2007, discussed at question 7.1, prohibits an individual or organization from sending unsolicited commercial electronic messages, such as emails and text messages. A company must have previously obtained the recipient's consent (express, or in some circumstances deemed) to receive commercial electronic messages. Such messages must also include a functional and free of charge unsubscribe function.

The ASA's Advertising Standards Code contains a similar rule in relation to personalized direct advertising. Advertisers must obtain appropriate consent from individuals before engaging in personalized direct advertising communications. Guidelines published by the ASA in relation to this rule stipulate that it must be clear to the recipient how they can unsubscribe or opt out. See question 7.5.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

When using vendors and other third parties in advertising, the information privacy principles relating to the collection, use and disclosure of personal information and the use of unique identifiers, will apply. However, to the extent the data being used is anonymized or de-identified, it will fall into an exemption under the Privacy Act and the information privacy principles will not apply.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The information privacy principles mentioned above at question 4.1 under the Privacy Act must be followed by agencies when collecting, using and storing an individual's personal information. Pursuant to these principles, when a business gathers information about an individual they must:

- (a) obtain permission from the individual to do so;
- (b) be clear about what they are gathering and what they will use it for;
- (c) not share personal information without the individual's knowledge or approval unless an exception applies;
- (d) inform the individual of their right to access the information and, if necessary, correct that information if it is incorrect or out of date; and
- (e) ensure the information is accurate and kept securely. When the business no longer needs the information, they must safely destroy it.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

There are several situations where agencies are expected to undertake diligence in their privacy practices to ensure ongoing compliance. These include:

- (a) If an agency wishes to provide a customer's personal information to an overseas third party (where permitted under the Privacy Act), it must undertake appropriate due diligence on that third party to confirm that either it is subject to privacy laws that, overall, provide comparable

- safeguards to those in the Privacy Act, or the third-party is otherwise required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act.
- (b) Under Privacy Principle 9 personal information should not be held for more than the time required for the purposes for which it may be lawfully used, and agencies should review their retention policies to ensure this is being complied with.

Undertaking a privacy impact assessment is not specifically required by the Privacy Act. However, it can be a useful process to go through to identify any issues early, making them easier to address.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Privacy Act primarily regulates direct marketing communications from a privacy perspective. Generally, marketers must tell consumers in clear, simple language what information about them is being collected, what it will be used for, who it will be disclosed to (if anyone) and that the customer has the right to access and correct their own information.

The Unsolicited Electronic Messages Act 2007 provides that an individual or organization that sends commercial electronic messages, such as emails and text messages, must notify the recipient of who the sender is and how to contact them. The message must also include a functional and free of charge unsubscribe function.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

If a business intends to use cookies, or other tracking technologies, on websites or apps to collect information about consumers, then the business should clearly notify consumers that such technologies are in use, how they are used (ie, what personal information is being collected and what it will be used for) and obtain consent.

7.3 How are loyalty programs and promotions regulated under privacy law?

There is no specific New Zealand legislation that governs loyalty programs and promotional activities from a privacy perspective. In order to comply with the information privacy principles, businesses should provide all participants of loyalty programs and promotions with a copy of its privacy policy. This should include accurate information about:

- (a) what personal information the business will collect;
- (b) what it will be used for;
- (c) how it will be securely stored;
- (d) whether it may be disclosed or shared (including with third parties, online, and overseas); and
- (e) how the individual can access and correct the information.

Personal information used for these programs or promotional offers cannot be kept longer than is required for its lawful use.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing is mainly regulated from a privacy perspective by the provisions of the Privacy Act. The information privacy principles give individuals the right to know what information about them is being collected, what it will be used for and who (if anyone) it will be

disclosed to, as well as the right to be informed of their ability to access and correct their information. In relation to text messages, emails, or direct messages, social media platforms will be subject to the provisions of the Unsolicited Electronic Messages Act 2007 as referred to above in response to question 7.1.

Overseas agencies who are doing business in New Zealand are subject to the Privacy Act. This means the Privacy Act, including the information privacy principles, apply to social media platforms operating in New Zealand. The Privacy Commissioner has the power to issue a compliance notice to social media platforms found to not be complying with New Zealand's privacy laws. Compliance notices would be enforceable in the Human Rights Review Tribunal and if a platform does not comply, it could face costs, as well as a fine of up to NZ \$10,000.

Social media advertising and influencer marketing is also subject to ASA's Advertising Standards Code which contains rules relating to privacy. See questions 5.2 and 7.5.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

In addition to the information privacy principles under the Privacy Act regarding collection, purpose, and disclosure (if any) of personal information, the ASA's Advertising Standards Code requires that advertisers obtain appropriate consent from consumers before engaging in personalized direct advertising communications. The following guidelines are to be followed by advertisers in interpreting that rule:

- (a) Personal information that is publicly available may be used for personalized direct advertising communications, providing that the information is not accompanied by a statement to the effect the person does not wish to receive such advertising;
- (b) Private personal information may be used for personalized direct advertising communications providing that consent has been obtained from the person to collect, store, and use their information for a defined purpose and the information collected is only used for that purpose; and
- (c) It must be clear to the recipient of any personalized direct advertising communication how they can unsubscribe or opt-out.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

The Privacy Act contains specific provisions relating to data matching between certain public sector agencies (provided that a number of rules are adhered to), but not in relation to data matching and digital identity resolution in the private sector. As a result, the use of these technologies is, for the most part, regulated by the information privacy principles relating to the collection, use and disclosure of personal information and the use of unique identifiers.

Generally, advertisers cannot disclose personal information to a third party without a legal basis to do so (eg, that the disclosure of the information is one of the purposes or is directly related to the purposes in connection with which the information was obtained). The Privacy Act does permit the disclosure of personal information where that personal information has been successfully de-identified (see question 3.3). If information is shared between an advertiser and a third party, the permitted uses of that information by each party needs to be considered, as well as the security of the information.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is, in general, regulated by the information privacy principles relating to the collection, use, and disclosure of personal information. Location data, to the extent to which it is personal information, may only be used for the purpose for which the individual was advised it was collected (with some limited exceptions, such as if it is used in a form in which the individual is not identified). To the extent that an individual's location data is provided to a third party for advertising purposes, permitted grounds for disclosure must exist (such as if the information has been de-identified). The rules relating to direct marketing communications in the ASA's Advertising Standards Code may also apply to location-based advertising to the extent that this involves personalized direct advertising communications. See question 7.5.

7.8 How are data brokers defined and regulated under privacy law?

Currently, there is no definition of 'data broker' in the Privacy Act and there are no specific laws or regulations in New Zealand governing the operation of data brokers.

Under the Privacy Act, an agency is exempt from the requirement to collect information directly from the individual concerned if the agency believes, on reasonable grounds, that the information is publicly available. However, if individuals do not have the right and the means to know which data brokers have information about them for marketing purposes or to see what information is being collected and how it is being used, then it is possible that collection of personal information by data brokers could be considered unfair or intrusive to an unreasonable extent upon the personal affairs of the individual concerned (particularly for children and other vulnerable consumers). This would amount to a breach of the Privacy Act.

7.9 How is advertising to children and minors regulated under privacy law?

The Privacy Act, in some instances, specifies how personal information must be treated with reference to the circumstances of the individual concerned. For example, privacy principle 4, which relates to how information must be collected, specifically highlights collection from children/ young people as a consideration. See question 3.2.

The ASA recognizes the sensitivity of personal information relating to children in its Children's Advertising Code, which includes a rule that extreme care must be taken when recording or requesting the personal details of children and young people to ensure that their privacy is protected, and that the information is not used in an inappropriate manner. The associated guidelines include that if an advertisement indicates that personal information about a child will be collected, this must include a statement that a parent's or guardian's consent is required. The advertiser must also not collect more information from a child than that which is needed for the relevant activity.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The Privacy Act does not contain specific provisions relating to profiling, the use of artificial intelligence or automated decision making. For the most part, this is regulated by the information privacy principles relating to the collection, use, disclosure and accuracy of personal information and the use of unique identifiers.

Under information privacy principle 8, an agency holding personal information should not use that information without taking any steps that are reasonable in the circumstances, to ensure that the information is accurate, up to date, complete, relevant and not misleading. The obligation to ensure information is accurate would also apply to any information generated about an identifiable person using artificial intelligence. Where using personal information to train artificial intelligence tools, consideration should also be given to the permitted use for which the personal information is collected.

7.11 Are there other specific advertising practices that you wish to discuss?

The use of biometric information to target advertising is an area of concern for the Privacy Commissioner, such as smart billboards that use shoppers' biometric information to target advertising. The draft Biometric Processing Privacy Code is intended to address concerns in this area.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The handling of 'personal information' (as defined in the Privacy Act) must comply with the Privacy Act's information privacy principles (see question 4.1). An agency must not transfer personal information to another organization except in compliance with the information privacy principles.

The Privacy Act prohibits the disclosure of personal information overseas unless an agency can be satisfied that one of the set criteria is satisfied—for example that:

- (a) the foreign person receiving the personal information is subject to privacy laws that, overall, provide comparable safeguards to those in New Zealand,
- (b) the individual concerned has given their informed consent to the disclosure, or
- (c) the agency transferring the information believes on reasonable grounds that the foreign organization receiving the personal information is required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act, such as pursuant to an agreement.

There are no specific countries or jurisdictions where transfer is prohibited. However, it will be more difficult to satisfy the set criteria if the information is to be transferred to a jurisdiction without comparable privacy safeguards. The Privacy Commissioner may also issue a transfer prohibition notice, prohibiting the transfer of personal information as set out in the notice.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The Privacy Act outlines that where a person that is storing or processing information for another uses or discloses such information for its own purposes, it will be held accountable and treated as holding the information. This will be the case even if the company is not situated in New Zealand. Similarly, an agency remains accountable for information held by another person as its agent.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in New Zealand? Are there minimum standards? Does this differ by sector or size of the entity?

- (a) Data security is primarily regulated by the Privacy Act and its information privacy principles. As mentioned above at question 4.1, these core principles protect people's privacy by governing the collection, storage, and use of personal information, while also providing for legitimate use of information by government, businesses, and other organizations. In particular, principle 5 establishes the minimum standard for storage and security of personal information. That is, any agency that holds personal information must ensure that:
- (i) the information is protected by such security safeguards as it is reasonable in the circumstances to take against:
 - loss;
 - access, use, modification, or disclosure that is not authorized by the agency; and
 - other misuse; and
 - (ii) if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, the agency must do everything reasonably within its power to prevent unauthorized use or disclosure of the information.
- (b) Any organization holding data on identifiable individuals is required to appoint a privacy officer to monitor compliance with the Privacy Act and deal with privacy breaches. This requirement applies regardless of the size of the organization.
- (c) The codes of practice issued by the Privacy Commissioner impose additional obligations regarding securing data for certain sectors or classes of agencies, such as credit reporters and telecommunications providers.
- (d) There are also various standards, guides, manuals and assessments that assist organizations in addressing data security standards imposed by the Privacy Act and codes of practice, such as:
- (i) ISO/IEC 27001:2024 standard—this specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system for all organizations. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization;
 - (ii) The Protective Security Requirements—these outline the Government's expectations for managing personnel, physical and information security. They also include the New Zealand Information Security Manual, which is intended to assist not only government departments and agencies and their service providers, but also private sector organizations; and
 - (iii) Digital Government NZ: Risk Assessment Process—the Government has also developed a generic security risk assessment process intended to assist companies with ensuring that they meet the requirement to have a robust risk assessment process.

9.2 How are personal data breaches regulated in New Zealand? What are the requirements for notification and response?

Under the Privacy Act, data breaches are regulated through mandatory breach reporting requirements.

An agency must notify both the affected individual and the Privacy Commissioner as soon as practicable after becoming aware of a notifiable privacy breach (not every privacy breach will be notifiable). Where it is not reasonably practicable to notify the affected individual (ie, there is a large group of affected individuals), the agency must give public notice of the breach. There are some limited exceptions where an agency will not be required to notify an individual or give a public announcement of the breach (eg, where notification or public notice would endanger the safety of any person).

A privacy breach is notifiable if it is reasonable to believe that the breach has or is likely to cause serious harm to any of the affected individuals. Whether a privacy breach has caused or is likely to cause serious harm is assessed based on a range of factors, including:

- (a) the action taken to reduce harm;
- (b) the sensitivity of information;
- (c) the nature of harm which may be caused to individuals;
- (d) who obtained the information due to the breach; and
- (e) whether personal information is protected by a security measure.

Failing to notify the Privacy Commissioner of any notifiable breach is an offence and can result in a fine up to NZ\$10,000.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) If there is a breach of one or more information privacy principles, an individual can make a complaint to the Privacy Commissioner. If the matter is not able to be resolved, and the Privacy Commissioner considers that there has been an 'interference with privacy', the Privacy Commissioner may then refer the complaint to the Director of Human Rights Proceedings. If the Privacy Commissioner does not refer the matter to the Director of Human Rights Proceedings, the individual may bring the case directly to the Human Rights Tribunal. The Tribunal may issue a compliance notice, ordering that an agency does (or does not do) something and/or award the complainant with compensation.
- (b) Further, a person commits an offence under the Privacy Act and is liable upon conviction for up to NZ \$10,000 for:
 - (i) obstructing or not complying with the Privacy Commissioner in the exercise its power under the Privacy Act;
 - (ii) knowingly misleading the Commissioner to exercise its powers under the Privacy Act;
 - (iii) misrepresenting their authority under the Privacy Act;
 - (iv) misleading an agency to obtain access to someone else's personal information; or
 - (v) destroying a document containing personal information, knowing a request has been made for it.
- (c) There are various statutes which prohibit certain types of intrusion (eg, using devices to monitor private conversations, or opening a letter addressed to another person) and which create offenses in order to protect a person's privacy interest and prevent the disclosure of certain information.

10.2 Do consumers have a private right of action? What remedies are available to them?

- (a) Individuals may bring a common law claim for an invasion of privacy.
- (b) Individuals can seek an injunction to prevent invasion of their privacy.
- (c) General damages (for example, compensation for hurt and upset) and exemplary damages are also available as remedies.
- (d) As referred to above, an individual personally affected by a breach (or that individual's representative) may make a complaint to the Privacy Commissioner.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The Office of the Privacy Commissioner ('OPC') can initiate investigations on its own initiative. However, generally, its focus is on education and responding to interferences with privacy in respect of which it has received a complaint.

The ASA has a reactionary approach to enforcement. It responds to complaints raised by members of the public.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in New Zealand?

There are currently no specific privacy rules which relate to the culture of New Zealand. The proposed Biometric Processing Privacy Code, discussed at question 11.2, will introduce a requirement to consider cultural impacts and effects of biometric processing on Māori when assessing whether biometric processing is proportionate to the likely impact on the individual concerned. Under the draft Code, biometric information must not be collected unless, in the particular circumstances, the collecting agency believes on reasonable grounds that the biometric processing is proportionate to the likely impacts on the individual concerned. The OPC has recently established a Māori Reference Panel to guide its work. Māori are the indigenous peoples of New Zealand.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

- (a) A developing area of interest is the use of biometric information. The OPC has stated that biometric information is personal information (and therefore governed by the Privacy Act). However, the OPC has also recognized that the Privacy Act framework does not cover all the issues posed by this topic. To address this, the Privacy Commissioner has announced their intention to issue a Biometric Processing Privacy Code. The draft Code suggests restrictions on businesses' use of biometric information that is currently set out in the information privacy principles.
- (b) To address a perceived gap in the Privacy Act, the New Zealand Government has proposed an amendment to that Act in the form of the Privacy Amendment Bill. While there is currently a requirement under the Privacy Act to inform individuals of various matters when collecting personal information directly from them, there is no corresponding requirement when information is collected indirectly. This Bill introduces a new information privacy principle 3A which will require an agency, if it collects personal information from a source other than from the individual to whom the information relates, to take reasonable steps to ensure that

individual is aware of the collection of that information, the purpose of collection and the intended recipients of the information, among other matters. The Bill as currently drafted provides some limited exceptions to these requirements, such as if the information is publicly available or compliance would reveal a trade secret.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

If you are processing personal data in New Zealand, we recommend that you seek specific New Zealand legal advice to ensure that you are complying with your privacy obligations in the context in which your business is operating.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

- (a) The new Biometric Processing Privacy Code and the Privacy Amendment Bill, discussed at question 11.2, are examples of recent changes in the privacy framework. The new Biometric Processing Privacy Code has been introduced to address shortcomings in the Privacy Act in relation to this emerging technology.
- (b) A new Consumer and Product Data Bill has also been introduced. This Bill seeks to establish a consumer data right in New Zealand. This follows the introduction of open-banking and consumer data rights in other jurisdictions, particularly the United Kingdom and Australia. The Bill as drafted will give customers the right to require one business to share their customer data with another trusted business. Initially, the legislation will only apply to the electricity and banking sectors.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

With the increasing inter-connectedness of companies and flow of data across borders, companies will need to ensure they remain compliant with privacy laws in not only their home jurisdiction, but with privacy laws and standards in other jurisdictions.

A challenge that may arise for some companies as technology continues to develop is the initial consent or permission obtained by that company to use personal data not keeping up with new ways that data can be used.

12.3 What do you envision the privacy landscape will look like in five years?

We expect that there may be developments in relation to emerging areas such as the use of artificial intelligence in decision making. We also expect the Biometric Processing Privacy Code will be progressed.

NICARAGUA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Nicaragua.

In Nicaragua, privacy is regulated by Law No 787 on the Protection of Personal Data, which was approved by the legislative branch on March 21, 2012 and came into effect upon publication in the Official Journal on March 29, 2012.

This law regulates the processing of personal data relating both to natural persons and legal entities, regardless of whether it is carried out by automated means or not. The objective of this law is to guarantee the right to personal and family privacy, as well as the right to information self-determination.

1.2 What are the primary laws regulating privacy in Nicaragua? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Key laws are:

- (a) the Law on the Protection of Personal Data; and
- (b) Regulations to the Law on the Protection of Personal Data (Decree 36-2012), in force since October 17, 2012.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In Nicaragua, self-regulation plays a rather limited role. There is a self-regulation code which specifically regulates advertising in the alcohol industry, in which there is an emphasis on regulating such advertising so that it does not encourage drinking in minors or associate any type of behavior with the consumption of alcoholic beverages.

However, at present we do not have a self-regulation code in connection with privacy regulation, nor a self-regulatory body.

1.4 How is privacy law enforced in Nicaragua? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Law on the Protection of Personal Data provides for the creation of a Directorate for Personal Data Protection within the Ministry of Finance and Public Credit. This Directorate will be in charge of many data-protection-related activities, such as operating a database registry, issuing regulations, monitoring compliance, as well as imposing administrative sanctions (in cases of violations). However, the Directorate has not yet been created, and, therefore, the Law is not fully applicable, as it is not possible to comply with certain of its requirements, such as registering in the Directorate's database. Furthermore, administrative sanctions (in cases of violations) cannot be imposed and there is currently no entity in charge of monitoring compliance.

Furthermore, at present, we do not have a self-regulation code in connection with privacy regulation, nor a self-regulatory body.

Thus, privacy law enforcement in Nicaragua is fragmented and relies on constitutional protections and general legal principles. The lack of a dedicated privacy regulator creates challenges, but individuals and companies can still take steps to protect privacy rights and comply with existing obligations as much as possible.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Nicaragua?

In Nicaragua, companies are subject to privacy laws primarily based on how they handle personal data and whether they fall under the scope of the country's data protection regulations. The key factors that make a company subject to privacy laws in Nicaragua can be summarized as follows:

- (a) **Handling of personal data:** Companies that collect, process, store, or transfer personal data of individuals (eg, customers, employees, or other stakeholders) are subject to privacy regulations.
'Personal data' includes any information that can identify an individual, such as names, addresses, ID numbers, phone numbers, email addresses, or financial information.
- (b) **Operations in Nicaragua:** Companies physically located or operating in Nicaragua are subject to local laws, including privacy-related provisions.
Foreign companies with a presence in Nicaragua (eg, subsidiaries, branches, or representatives) are also subject to Nicaraguan privacy laws if they process personal data of Nicaraguan residents.
- (c) **Compliance with the Nicaraguan Constitution:** The Nicaraguan Constitution guarantees the right to privacy and the protection of personal data. Companies must respect this constitutional right when handling individuals' information.
- (d) **Contractual obligations:** Companies that enter into contracts with individuals or other entities may be bound by privacy clauses or confidentiality agreements that require compliance with data protection principles.
- (e) **General legal principles:** Companies are expected to adhere to general legal principles of fairness, transparency, and accountability when handling personal data. Failure to do so could result in legal liability under civil or criminal law.

2.2 Does privacy law in Nicaragua apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

No. It does not apply to foreign companies that do not have local presence in the country.

However, foreign companies with a presence in Nicaragua (eg, subsidiaries, branches, or representatives), which process personal data of Nicaraguan residents, are also subject to the applicable Nicaraguan privacy laws.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Nicaragua?

'Personal data' under privacy law is defined as any information relating to an identified or identifiable natural persons or legal entities.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

According to Nicaraguan law, 'sensitive personal data' is all information that reveals the racial, ethnic, political affiliation, religion, philosophical or moral creed, union membership, health data, sexual preferences, criminal or administrative records, financial information, and any other information that may be grounds for discrimination.

Sensitive personal data can only be obtained and processed for reasons of general interest, with the consent of the owner of the data, or through a court order. It may also be treated for statistical or scientific purposes when their holders cannot be identified. Personal data, relating to criminal records or administrative offenses, can only be processed by the competent public authorities.

Personal data related to health, in hospitals, clinics, public and private health centers and professionals linked to health can only refer to the physical or mental health of patients, preserving professional confidentiality.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The Law on the Protection of Personal Data does not specifically address anonymized, pseudonymized, or de-identified data. However, the treatment of such data can be inferred from general legal principles, constitutional protections, and international best practices that may influence Nicaraguan law.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) **Notice:** Data subjects should be given notice when their data is being collected as well as contact information for the entity collecting the data;
- (b) **Purpose:** Data subjects must be informed about the purposes for which their data will be used and whether it is voluntary or mandatory to provide the information;
When it no longer serves the purpose for which it was collected, personal information should be deleted;
The information collected should only be used for the purpose stated and not for any other purposes. If there is a change from the purpose for which the information was originally collected, the individual must be informed by the entity collecting it;
- (c) **Consent:** Consent, where required, must be obtained in advance of collection/processing and must be freely given. As a general rule, tacit consent is valid. However, for purposes of processing financial data or other sensitive information, express consent is required;
- (d) **Security:** The collected data should be kept secured from any potential abuse. As a result, the entity collecting the data must take appropriate technical measures to prevent any unauthorized access to or use of the information;
- (e) **Disclosure:** Data subjects should be informed as to who is collecting their data;
- (f) **Access:** Data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- (g) **Accountability:** Data subjects should have a method available to them to hold data collectors accountable for following the principles outlined above.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No. The law in Nicaragua does not assign different roles to companies based on how they process personal data. Nevertheless, companies can infer responsibilities from general legal principles and international standards:

- (a) A data controller has the following obligations:
 - (i) **Determine purpose and means:** to decide why and how personal data is processed;
 - (ii) **Transparency:** to inform individuals about data collection and processing activities (eg, through privacy notices);
 - (iii) **Lawful basis for processing:** to ensure there is a valid legal basis for processing personal data, such as consent or contractual necessity;
 - (iv) **Data subject rights:** to respect individuals' rights, such as access, rectification, and erasure, even if not explicitly mandated by Nicaraguan law;
 - (v) **Data security:** to implement appropriate technical and organizational measures to protect personal data; and
 - (vi) **Accountability:** to maintain records of data processing activities and demonstrate compliance with privacy principles.
- (b) A data processor has the following obligations:
 - (i) **Act on instructions:** to process personal data only as instructed by the controller;
 - (ii) **Data security:** to implement security measures to protect the data they process;
 - (iii) **Confidentiality:** to ensure that employees or subcontractors handling the data are bound by confidentiality obligations;
 - (iv) **Assist the controller:** to help the controller fulfill its obligations, such as responding to data subject requests or notifying breaches; and
 - (v) **Subcontracting:** if using subcontractors, to ensure they meet the same data protection standards.

While Nicaraguan law does not explicitly assign roles like 'controller' and 'processor,' companies should proactively adopt these concepts based on international best practices. By clearly defining roles and responsibilities, companies can better manage their data processing activities, reduce legal risks, and build trust with customers.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

No. The law in Nicaragua does not explicitly require a lawful basis for processing personal data, such as consent, legitimate interest, or contractual necessity. However, privacy-related obligations can be inferred from the Nicaraguan Constitution, general legal principles, and international best practices.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

While Nicaraguan law does not explicitly mandate the content of privacy notices, companies should adopt international best practices to ensure transparency and build trust with users. A well-crafted privacy notice for advertising purposes should clearly explain what data is collected, why it is used,

how it is shared, and how individuals can exercise their rights. This approach not only aligns with global standards but also helps companies mitigate legal and reputational risks.

The recommended information to include in privacy notice includes:

- (a) identity and contact information;
- (b) purposes of processing;
- (c) types of personal data processed;
- (d) consent;
- (e) data retention period;
- (f) individual rights;
- (g) opt-out mechanisms; and
- (h) contact for privacy concerns.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the following privacy rights:

- (a) Right of access and rectification;
- (b) Right to erasure;
- (c) Right to withdraw consent;
- (d) Data portability;
- (e) Right to restriction of processing; and
- (f) Right to lodge a complaint with the regulatory authority.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

The Nicaraguan privacy law does not have a specific mechanism to obtain consent or opt-out options for advertising activities. However, companies can adapt international best practices and general principles of fairness and transparency to guide their approach:

(a) Consent

(i) Consent is typically required in the following circumstances:

- the advertising involves the processing of sensitive personal data (eg, health information, religious beliefs), explicit consent is generally required;
- the advertising is not necessary for the performance of a contract or another lawful basis (eg, legitimate interest), consent is often the appropriate justification;
- personal data is shared with third parties (eg, advertising networks, social media platforms) for targeted advertising, consent is usually required; or
- cookies, pixels, or other tracking technologies are used for behavioral advertising, consent is typically necessary.

(ii) When obtaining consent:

- consent requests must be clear, specific, and separate from other terms and conditions;
- individuals should be provided with granular choices (eg, opt-in for different types of advertising);

- make it easy for individuals to withdraw consent at any time (eg, through an unsubscribe link or preference center); and
 - maintain records of consent obtained, including when and how it was given.
- (b) **Opting out**
- (i) Opt-out options are generally required in the following circumstances:
- if the company relies on legitimate interest as the lawful basis for advertising, individuals must have the right to object (opt out);
 - for email marketing campaigns, providing an opt-out option is required by the Nicaraguan Law;
 - if personal data is shared with third parties for advertising, individuals should have the option to opt out of such sharing; or
 - if cookies or tracking technologies are used for targeted advertising, individuals should be able to opt out of such tracking.
- (ii) Providing opt-out options:
- include an easy-to-use unsubscribe link in all marketing emails;
 - allow individuals to manage their advertising preferences through a user-friendly preference center; and
 - provide a cookie banner or pop-up that allows users to opt out of non-essential cookies and tracking.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The Law on the Protection of Personal Data in Nicaragua has not been fully implemented or enforced due to the lack of regulatory development and the absence of a designated regulatory authority. However, the law does provide a framework for the protection of personal data, and whilst it does not explicitly address the use of vendors and third parties in advertising, it includes provisions that could apply in such cases:

- (a) Key considerations when sharing with third parties include:
- (i) **Consent for data sharing:** If personal data is shared with third parties (eg, advertising agencies, DSPs, SSPs, or data providers), the data subject must be informed, and their explicit consent must be obtained, unless another lawful basis applies.
- (ii) **Transparency:** Companies must clearly disclose the types of third parties involved, the purposes of data sharing, and how the data will be used.
- (b) When using third parties for advertising purposes, companies should consider:
- (i) **Consent for targeted advertising:** If personal data is used for targeted advertising (eg, through cookies or tracking technologies), companies must obtain explicit consent from individuals;
- (ii) **Transparency and information:** Individuals must be informed about the use of their data for advertising and provided with an easy way to opt out; and
- (iii) **Data minimization:** Companies should only share the minimum amount of personal data necessary for the advertising purpose.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The Nicaraguan privacy law does not explicitly mandate contractual obligations for data sharing. Therefore, companies should adopt international best practices to ensure compliance with privacy principles. By implementing robust data processing agreements ('DPA's), companies can define the roles and responsibilities of third parties, protect personal data, and mitigate legal risks.

Key clauses would include:

- (a) the purpose and scope of data processing;
- (b) the obligations of the third party to protect personal data;
- (c) prohibition on using the data for unauthorized purposes;
- (d) requirements for notifying the company in case of a data breach; and
- (e) rules for subcontracting (if applicable).

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

- (a) **Due diligence:** While the Law on the Protection of Personal Data does not explicitly outline due diligence measures, its general principles and obligations imply that companies should take the following steps to ensure compliance:
 - (i) **Transparency and information**
 - Companies must inform individuals about the collection, use, and processing of their personal data, including the purposes and legal bases for processing;
 - Obtain explicit consent from individuals before processing their personal data, unless another lawful basis applies;
 - (ii) **Data security**
 - Implement appropriate measures to protect personal data from unauthorized access, loss, or destruction;
 - Regularly assess and address security risks to ensure the confidentiality, integrity, and availability of personal data;
 - (iii) **Third party management**
 - Evaluate the data protection practices of third parties (eg, advertising agencies, DSPs, SSPs) before sharing personal data;
 - Ensure that third parties are bound by contracts that include data protection obligations, such as confidentiality, security, and compliance with the Law on the Protection of Personal Data;
 - (iv) **Data subject rights**
 - Establish procedures to respond to individuals' requests to access, correct, or delete their personal data;
 - Allow individuals to object to processing or withdraw consent at any time;
 - (v) **Record keeping**
 - Maintain records of data processing activities, including the purposes of processing, categories of data, and third parties involved;
 - Regularly review and update privacy practices to ensure ongoing compliance with the Law on the Protection of Personal Data.

- (b) **Impact assessments for advertising uses:** The Law on the Protection of Personal Data does not explicitly require data protection impact assessments ('DPIA's). However, the principles of accountability and risk management suggest that companies should conduct DPIAs for high-risk processing activities, such as:
- (i) **Targeted advertising:** If advertising involves profiling or tracking individuals' behavior (eg, using cookies, pixels, or other tracking technologies), a DPIA may be required to assess the risks to individuals' privacy;
 - (ii) **Sensitive data:** If advertising involves the use of sensitive personal data (eg, health information, religious beliefs), a DPIA is recommended to evaluate the potential impact on individuals;
 - (iii) **Mass data collection:** If advertising activities involve the large-scale collection or processing of personal data (eg, through programmatic advertising), a DPIA can help identify and mitigate risks;
 - (iv) **Innovative advertising techniques:** If using new technologies or methods for advertising (eg, AI-driven targeting), a DPIA is advisable to assess potential privacy risks; and
 - (v) **Cross-border data sharing:** If personal data is transferred to third parties or advertising partners outside Nicaragua, a DPIA can help evaluate the adequacy of data protection safeguards.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications may only incorporate personal data with the consent of the owner, unless the data was obtained from a publicly-accessible source.

The owner of the data may exercise the right of access without charge, and may, at any time, request the deletion of their data files.

The entity conducting the marketing communications must offer the data owner the chance to express their refusal to continue receiving such materials or, where appropriate, to revoke their consent in a clear manner and at no cost to the data owner.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies is not regulated. Once the Directorate for Personal Data Protection is created, this body will be able to draft specific regulations in such regard.

7.3 How are loyalty programs and promotions regulated under privacy law?

According to the Law on the Protection of Personal Data, data subjects should be informed of their rights over such data, the source from which the data was obtained and the entity responsible for handling the data. The personal data can only be incorporated with the owner's consent unless obtained from a publicly-accessible source.

The owner of the data may exercise the right of access without charge, and may, at any time, request the deletion of their data files.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing often involve the collection and processing of personal data, such as user profiles, engagement metrics, and behavioral data.

(a) Applying the requirements in the Law on the Protection of Personal Data to these activities:

(i) **Consent for data collection**

- If personal data is collected from social media users (eg, through contests, giveaways, surveys, tracking tools or direct messaging), companies and influencers must obtain explicit consent from individuals;
- Individuals must be informed about the purposes of data collection (eg, for targeted advertising or influencer campaigns) and how their data will be used;

(ii) **Transparency in marketing practices**

- Influencers and brands must clearly disclose any commercial relationships or sponsorships in their social media posts (eg, using hashtags like #ad or #sponsored) and avoid misleading their audience about the nature of sponsored content;
- Provide clear and accessible privacy notices that explain how personal data is used in social media and influencer marketing;

(iii) **Data minimization**

- Only collect the personal data necessary for the marketing campaign (eg, avoid collecting excessive or irrelevant data);
- Where possible, use anonymized or aggregated data for analytics and targeting;

(iv) **Data security**

- Implement security measures to protect personal data collected through social media platforms or influencer campaigns (eg, encryption, access controls);
- Ensure that any third-party tools or platforms used for social media marketing comply with data protection principles;

(v) **Respect for user rights**

- Allow individuals to access and correct their personal data used in marketing campaigns;
- Provide users with the option to object to the use of their data for marketing purposes or to opt out of targeted advertising.

In addition, companies using social media platforms for advertising must:

- (vi) adhere to the privacy policies and terms of service of social media platforms;
- (vii) ensure that any data collected through social media ads (eg, via tracking pixels) is done with user consent; and
- (viii) avoid using sensitive personal data (eg, health information, religious beliefs) for targeted advertising without explicit consent.

(b) **Practical recommendations for compliance**

While the Law on the Protection of Personal Data is not fully enforced, companies and influencers should adopt the following measures to ensure compliance with its principles:

- (i) Companies
 - create privacy policies that explain how personal data is used in social media and influencer marketing;
 - use clear and unambiguous consent mechanisms (eg, opt-in checkboxes) for data collection;
 - educate influencers on their responsibilities regarding data protection and transparency; and
 - regularly review social media campaigns to ensure compliance with privacy principles.
- (ii) Influencers
 - clearly disclose sponsored content and commercial relationships;
 - avoid collecting or sharing personal data without consent; and
 - adhere to the terms of service and community guidelines of social media platforms.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There is no specific regulation for targeted advertising and behavioral advertising. Once the Directorate for Personal Data Protection is created, this body will be able to draft specific regulations in such regard.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There is no specific regulation for digital identity resolution and clean room technologies under the Nicaraguan privacy law. Once the Directorate for Personal Data Protection is created, this body will be able to draft specific regulations in such regard.

7.7 How is location-based advertising regulated under privacy law?

There is no specific regulation for location-based advertising. Once the Directorate for Personal Data Protection is created, this body will be able to draft specific regulations in such regard.

7.8 How are data brokers defined and regulated under privacy law?

While the Law on the Protection of Personal Data does not explicitly define data brokers, they can be understood as entities that collect, aggregate, and sell or share personal data obtained from various sources. Data brokers typically operate as intermediaries between data collectors (eg, websites, apps) and data users (eg, advertisers, marketers).

Data brokers must:

- (a) take the necessary safety measures;
- (b) keep data confidential; and
- (c) obtain registration.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors involves additional considerations due to their vulnerability and the need for enhanced protection. Below is how the Law on the Protection of Personal Data might apply:

- (a) **Consent for data collection:** If personal data is collected from children (under the age of 18), companies must obtain parental consent before processing the data.
- (b) **Transparency:** Provide clear and accessible privacy notices that explain the use of personal data for advertising purposes; and use language that is easy for children and minors to understand.
- (c) **Data minimization:** Only collect the personal data necessary for the specified purpose.
- (d) **Data security:** Implement robust security measures to protect personal data from unauthorized access, loss, or misuse (eg, encryption, access controls).
- (e) **Respect for user rights:** Allow children and minors (or their parents) to access and correct their personal data used for advertising; and provide children and minors (or their parents) with the option to object to the use of their data for advertising or to opt out of targeted ads.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There is no specific regulation for profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes. Once the Directorate for Personal Data Protection is created, this body will be able to draft specific regulations in such regard.

7.11 Are there other specific advertising practices that you wish to discuss?

Not currently.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Please note that the Nicaraguan Law on the Protection of Personal Data states that personal data may only be transferred to third countries if that country provides an adequate level of protection. However, it does not specify what constitutes an adequate level of protection. As such, it would be the regulatory authority, the Directorate for Personal Data Protection—which has yet to be created—that would establish the norms concerning the minimum standards of adequate level of protection.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Not at present.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Nicaragua? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is regulated by the Law on the Protection of Personal Data, which states that data controllers must adopt the necessary technical and organizational measures to guarantee the integrity, confidentiality and security of personal data to prevent their adulteration, loss, consultation, treatment, disclosure, transfer or unauthorized disclosure, and to detect international deviations or not of private information, whether the risks come from human action or from the technical means used.

Additionally, the law provides for the Directorate for Personal Data Protection to implement the required regulations. However, given that such directorate has yet to be created, there are no particular standards in place for securing data.

9.2 How are personal data breaches regulated in Nicaragua? What are the requirements for notification and response?

At present, due to the fact that the competent authority (Directorate for Personal Data Protection) has yet to be created, for all practical purposes data breaches are not being regulated.

However, the Nicaragua law establishes that breaches may be minor or serious, and the following sanctions are contemplated:

- (a) suspension of operations related to the processing of personal data; and
- (b) the temporary or permanent closure or cancellation of the data controller's operations.

According to the Law on Protection of Personal Data and its Regulations, the owners of data have the right to be notified of any adulteration, loss, consultation, treatment, disclosure, transfer or unauthorized disclosure of their data.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) Suspension of operations related to the processing of personal data;
- (b) Closure or cancellation of the data controller's operations, temporarily or permanently; and
- (c) Compensation by way of damages.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes. According to the Law on Protection of Personal Data, the owner of the data may file a personal data protection action before the governing body (Directorate of Personal Data Protection). However, such action is not available at present as the Directorate of Personal Data Protection has yet to be created.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Nicaragua does not have an active enforcement regime for privacy-related matters, primarily because the Law on the Protection of Personal Data has not been fully implemented or enforced. The law, enacted in 2012, lacks the necessary designated supervisory authority to oversee compliance and enforce its provisions. As a result, there are no publicly reported examples of enforcement actions or lawsuits specifically related to privacy non-compliance in advertising or other areas.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Nicaragua?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Companies should monitor whether the Nicaraguan government takes steps to fully implement the Law on the Protection of Personal Data, including the establishment of a supervisory authority and the issuance of implementing regulations.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Not currently.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There have been no significant changes in Nicaragua’s privacy landscape since this book was last published in 2022: the Law on the Protection of Personal Data remains unimplemented due to the lack of regulatory development and a designated supervisory authority.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

At this time, there are no changes in privacy landscape in Nicaragua.

12.3 What do you envision the privacy landscape will look like in five years?

Nicaragua’s privacy landscape is likely to evolve significantly, driven by global trends, technological advancements, and increasing consumer awareness. While the full implementation of the Law on the Protection of Personal Data remains uncertain, companies should proactively adopt best practices and prepare for potential regulatory changes. By staying informed about global and regional developments, implementing robust data protection measures, and fostering a culture of privacy, companies can navigate the evolving landscape effectively and build trust with consumers.

 NIGERIA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Nigeria.

Nigeria does not have a principal data and privacy protection law. However, the Constitution of the Federal Republic of Nigeria 1999 (as amended in 2011) ('the Constitution') provides protection for the right to private life. In 2019, the Nigerian legislature passed the Nigeria Data Protection Regulations 2019 ('NDPR') into law, and these Regulations were issued by the National Information Technology Development Agency ('NITDA') on January 25, 2019, pursuant to the National Information Technology Development Agency Act 2007. On June 12, 2023 the Nigeria Data Protection Act 2023 ('NDPA') was signed into law by the current President of the Federal Republic of Nigeria, President Bola Ahmed Tinubu, to further strengthen the data protection regime in Nigeria.

1.2 What are the primary laws regulating privacy in Nigeria? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

See question 1.1.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Nigerian Code of Advertising is the primary regulatory framework governing advertising, sales promotions, and marketing communications in Nigeria. Issued by the Advertising Regulatory Council of Nigeria ('ARCON'), the code ensures that all advertisements are legal, decent, honest, and respectful of Nigerian culture. It sets guidelines on the presentation of ads, prohibits misleading claims, and establishes rules for specific product categories, including alcohol, tobacco, and pharmaceuticals. The code also provides a mechanism for vetting advertisements and imposes sanctions for violations, ensuring transparency and accountability in the advertising industry.

1.4 How is privacy law enforced in Nigeria? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

When compared to developed nations, the Nigerian judiciary struggles with the notion of finding a balance between individual right to privacy claims and the need to uphold or reject the same. However, privacy laws in Nigeria may be enforced through a civil action in either the Federal High Court or State High Court by relying on the Constitution.

NITDA is the federal government agency responsible for regulating issues related to privacy and data protection in Nigeria. It is also charged with responsibility for setting up an Administrative Redress Panel whose duty it is to:

- (a) investigate allegations of breach of privacy;
- (b) conclude its investigations; and
- (c) determine, within 28 days, the appropriate redress.

The Nigeria Data Protection Commission ('NDPC'), on the other hand, is the primary regulatory authority responsible for overseeing data protection and privacy in Nigeria, established under the NDPA. The NDPC was created to replace the data protection oversight role previously held by NITDA, providing a more specialized and autonomous regulatory framework for data protection.

The NDPC is empowered to regulate the processing of personal data, ensure data security, and safeguard the privacy rights of individuals in Nigeria. Its functions include formulating data protection policies, issuing guidelines for data controllers and processors, conducting audits to ensure compliance, investigating data breaches, and imposing sanctions for non-compliance. The Commission also provides a framework for data breach notifications and promotes awareness of data protection rights among citizens.

Structured to operate independently, the NDPC is headed by a Commissioner and other appointed officials with clear mandates to uphold data protection standards across various sectors. It has the authority to license data protection compliance organizations ('DPCO's) that assist organizations in achieving compliance with data protection regulations. Through the NDPC, Nigeria aims to align its data protection framework with global standards, ensuring the responsible and secure handling of personal data in the digital age.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Nigeria?

Any company that does any of the following is subject to privacy laws:

- (a) processes personal data;
- (b) employs natural persons who reside in Nigeria, or who reside outside Nigeria but are of Nigerian descent; or
- (c) enters into any contract or agreement with a natural person or corporate entity in respect of issues protected by privacy laws.

2.2 Does privacy law in Nigeria apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Only the NDPR apply to businesses established in other jurisdictions. The NDPR apply to:

- (a) all transactions for the processing of personal data, regardless of the means by which the data processing is being or is intended to be conducted, in respect of natural persons in Nigeria, and
- (b) all natural persons residing outside Nigeria who are citizens of Nigeria.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Nigeria?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject').

An 'identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Such factor can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as, but not limited to, MAC address, IP address, International Mobile Equipment Identity ('IMEI') number, International Mobile Subscriber Identity ('IMSI') number, SIM and others.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive personal data’ is data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

The specific obligations around sensitive information include the responsibility of, and duty of care owed by, persons entrusted with such information to take extra care in order to secure such information against all foreseeable hazards and breaches, such as theft, cyber-attack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The NDPA does not provide a specific definition for ‘anonymized’ or ‘pseudonymized’ data. However, the Act encourages data controllers and processors to implement technical and organizational measures to protect personal data, including pseudonymization.

The NDPR provide that: ‘Anyone involved in data processing or the control of data shall develop security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data...’

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The NDPR provide that, for processing to be lawful, at least one of the following must apply:

- (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; and
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No. The NDPR does not distinguish between controllers and processors. It provides that EVERY data controller must:

- (a) make available to the general public their respective data protection policies;
- (b) designate a data protection officer for the purpose of ensuring adherence to the NDPR and other relevant data privacy instruments and data protection directives of the data controller

- (although a data controller may outsource data protection to a verifiably competent firm or person); and
- (c) ensure continuous capacity building for their data protection officers and the generality of their personnel involved in any form of data processing, etc.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes. The NDPR provide that 'No data shall be obtained except where the specific purpose of collection is made know to the data subject', and further provides that the data controller is under an obligation to ensure that consent of a data subject has been obtained without fraud, coercion or undue influence.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

There are no specific requirements under the privacy laws for data protection with respect to advertising. However, processing of personal data must be done lawfully, as the data processor owes the data subject a duty of care and will be accountable under the NDPR for their acts or omissions.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

We advise that the rights of consumers as provided under the NDPR do not specifically relate to the context of advertising. The following rights are available to consumers as regards their personal data:

- (a) right of access to data or copies of data;
- (b) right to rectification of records;
- (c) right to deletion or right to be forgotten;
- (d) right to restrict processing;
- (e) right to data portability;
- (f) right to withdraw consent;
- (g) right to object to marketing;
- (h) right to structured data;
- (i) right to make requests to the data controller without being charged; and
- (j) right to make a complaint to the data protection authority.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

There are no specific provisions in the NDPR concerning specific circumstances under which consent of data subjects must be obtained by the data controller in respect of advertising activities.

However, the consent of data subjects must first be sought and obtained by the data controller before personal data can be processed.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

There are no express provisions concerning this aspect of privacy laws in Nigeria.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The NDPR specifically include the situation where data is to be transferred to a third party as one of the circumstances in which consent of the data subject must first be obtained by the data controller.

They also provide that ‘data processing by a third party shall be governed by a written contract between the third party and the data controller.’ Accordingly, any person engaging a third party to process the data obtained from data subjects must ensure adherence to this requirement.

The above provisions imply that consent of the data subject must first be obtained before personal data can be transferred to a third party. Moreover, prior to collecting personal data from a data subject, the controller must provide the data subject with the legitimate interests pursued by the third party—ie, the intention of the third party, and the purpose of the data transfer must be communicated by the data controller to the data subject prior to the transfer.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

The NDPR provide that any party to any data processing contract, other than an individual data subject, must take reasonable measures to ensure the other party does not have a record of violating the principles set out in the NDPR. Accordingly, companies must ensure that they are accountable to NITDA or a reputable regulatory authority for data protection within or outside Nigeria. For these purposes, ‘parties’ include the directors, shareholders and employees of a contracting party.

Every data controller is liable for the actions or inactions of third parties who handle the personal data of data subjects.

Companies must take due diligence to ensure that the consent of the data subject has been obtained before processing data.

The privacy laws in Nigeria do not make express provision for impact assessments in advertising matters.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Nigerian Code of Advertising and other rights and restrictions on practice provide that customer information must not be transferred to any party except to the extent agreed with the consumer, as permitted or required by the Nigerian Communications Commission (‘NCC’) or other applicable laws or regulations.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There are no specific regulations concerning this subject matter in Nigeria.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific privacy regulations for loyalty programs and promotions under Nigerian law. However, we advise that the general provisions on privacy shall apply in this regard.

7.4 How is social media and influencer marketing regulated under privacy law?

The NDPA requires social media platforms, advertisers, and influencers to obtain lawful consent before collecting, processing, or sharing users' personal data for targeted ads or marketing campaigns.

The ARCON mandates that all social media advertisements, including influencer marketing, adhere to the Nigerian Code of Advertising. Influencers must disclose sponsored content to prevent misleading advertising.

Also, the Federal Competition and Consumer Protection Commission ('FCCPC') enforces fair marketing practices, ensuring that influencer endorsements are not deceptive and that personal data is not misused.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Privacy laws in Nigeria regulate targeted advertising, including behavioral and personalized advertising, by imposing data protection requirements. For example, the NDPA requires lawful consent before collecting and processing personal data for targeted adverts, it also grants individuals the right to opt-out of personalized advertising, and mandates transparency in how advertisers track and use consumer data.

Further to the above, the ARCON and the FCCPC prohibit deceptive or intrusive advertising practices, and enforce disclosure requirements for advert personalization and influencer marketing.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Not applicable.

7.7 How is location-based advertising regulated under privacy law?

There are no specific regulations concerning this subject matter.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific regulations in this regard.

7.9 How is advertising to children and minors regulated under privacy law?

The NDPR provide that data controllers must communicate any information relating to the processing of data in plain, clear and concise language particularly if such information is addressed to a child.

The NDPR also stipulate that, where the purpose of the processing of data is to propagate child rights violations, consent must not be sought, granted or accepted.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific regulations in this regard.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The regulations on data transfer in Nigeria under the NDPR provide that the transfer to foreign countries or international organizations of personal data already being processed or for purposes of processing must be done subject to the provisions of the NDPR, and under the supervision of the Honorable Attorney General of the Federation. Accordingly:

- (a) a transfer of personal data to a foreign country or an international organization will only be approved by the NITDA when the Agency is sure that the receiving country ensures an adequate level of protection;
- (b) the Attorney General will take into consideration the following issues:
 - (i) the legal protection for human rights and security of citizens in the foreign country;
 - (ii) the adequate protection of personal data through legislation, existence of caselaw on data protection, established rules for the transfer of personal data to foreign countries, and a viable judicial system of redress for data subjects;
 - (iii) the level of compliance with, and enforcement of, data protection laws; and
 - (iv) the international commitments of the foreign country or international organization concerned to legally-binding conventions or instruments on the protection of personal data.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a foreign country or to an international organization shall take place subject to the provisions of the NDPR and the supervision of the Honorable Attorney General of the Federation.

The transfer or a set of transfers of personal data to a foreign country or an international organization may take place only under one of the following conditions:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards, and that there are no alternatives;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;

- (e) the transfer is necessary for the establishment, exercise or defense of legal claims; and
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

In any case, the data subject must be clearly warned of the specific principle(s) of data protection that is likely to be violated in the event of transfer to a third country. This proviso does not apply to any instance where the data subject is answerable in a duly established legal action for any civil or criminal claim in a third country.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Nigeria? Are there minimum standards? Does this differ by sector or size of the entity?

Data security in Nigeria is regulated primarily under the NDPA, which mandates organizations to implement appropriate security measures (eg, encryption, access controls) to protect personal data from breaches, unauthorized access, and misuse. It also mandates data breach notification to the Nigeria Data Protection Commission ('NDPC') and affected individuals.

In addition, the Cybercrimes (Prohibition, Prevention, etc) Act 2015 criminalizes unauthorized data access, hacking, and identity theft, and further requires businesses, especially financial institutions, to implement cybersecurity safeguards.

Finally, we have industry-specific regulations such as:

- (a) the Central Bank of Nigeria Regulations, which regulate data security for banks and other financial institutions, and provide IT standards for data protection; and
- (b) the NCC Consumer Code of Practice Regulations 2024, which regulate telecoms operators in order to ensure network security and data privacy.

9.2 How are personal data breaches regulated in Nigeria? What are the requirements for notification and response?

Personal data breaches are regulated under the NDPA, which mandates organizations to take prompt action in response to data breaches.

Data controllers must notify the NDPC within 72 hours of becoming aware of a breach. If the breach poses a high risk to individuals' rights, affected persons must also be informed without undue delay.

Furthermore, organizations are required to investigate breaches and assess the impact, and they must also implement mitigation strategies to prevent further harm.

Failure to report or handle breaches properly can result in fines, sanctions, or reputational damage as provided under the NDPR.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Where a data controller has breached the data privacy rights of a data subject, the NDPR specifies the following penalties, in addition to any other criminal liability:

- (a) in the case of a data controller dealing with more than 10,000 data subjects, a fine of 2% of its annual gross revenue of the preceding year, or 10 million naira, whichever is greater;
- (b) in the case of a data controller dealing with less than 10,000 data subjects, a fine of 1% of its annual gross revenue of the preceding year, or 2 million naira, whichever is greater.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes. Consumers have a private right of action and may claim damages as compensation in a civil suit.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Quite active.

In July 2024, the FCCPC, in collaboration with the NDPC, fined Meta USD 220 million for multiple violations of Nigeria’s data protection and consumer rights laws. The investigation revealed that Meta had appropriated Nigerian users’ data without consent, enforced exploitative privacy policies, and treated Nigerian consumers unfairly compared to other regions.

In August 2024, the NDPC imposed a fine of approximately NGN 555,800,000 million (approx USD 358,580) on Fidelity Bank for breaches of the NDPA during the account opening process for a customer. The bank was found to have collected personal data without proper consent and misused tools like cookies and banking apps without obtaining informed user consent.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Nigeria?

Some cultural considerations significantly impact privacy law and enforcement in Nigeria. For example, certain religious and cultural practices involve public sharing of personal information (eg, in religious records, community announcements), sometimes conflicting with modern privacy principles.

Also, many Nigerians have limited awareness of data protection laws and their rights, leading to weaker enforcement and less public demand for privacy compliance.

Again, Nigeria has a strong communal culture, where family and community ties often lead to shared access to personal data (eg, banking details, health records). This often challenges strict individual consent models in the application of data protection laws in Nigeria.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Concerning hot topics, the Nigerian government is increasingly focused on enforcing data protection laws, and companies that fail to comply with the NDPA and NDPR may face fines or other penalties.

New technologies, such as artificial intelligence (‘AI’) and machine learning (‘ML’), are being used more and more in advertising. These technologies raise new privacy concerns, such as the use of personal data to target ads. Companies need to be aware of the privacy implications of using these technologies.

Many companies that advertise to Nigerian consumers are based outside of Nigeria. These companies need to be aware of the rules on cross-border data flows. The NDPA and NDPR restrict the transfer of personal data to countries that do not have adequate data protection laws.

With respect to challenges, we advise that companies should be careful about how they use personal data to target ads. The NDPA and NDPR require companies to obtain consent for the use of personal data for advertising purposes. Companies also need to be careful not to use sensitive personal data, such as health or religious information, for targeted advertising.

Companies need to be transparent about their use of cookies and other tracking technologies. The NDPR require companies to provide consumers with clear and conspicuous notice of the use of these technologies. Companies also need to give consumers the option to opt out of the use of these technologies.

Companies need to be aware of the privacy implications of using AI and ML in advertising. These technologies can be used to collect and process large amounts of personal data.

Companies need to be careful not to use these technologies in a way that discriminates against consumers or that violates their privacy rights

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The NDPA was signed into law by the current President of the Federal Republic of Nigeria, President Bola Ahmed Tinubu on June 12, 2023. Generally, we can say that the need to provide better legislation to safeguard personal data was responsible for triggering these changes.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The biggest challenges companies face due to the changing privacy landscape include:

- (a) keeping up with evolving data protection laws like the GDPR and the NDPA;
- (b) implementing robust security measures to prevent data breaches;
- (c) navigating complex rules on cross-border data transfers;
- (d) efficiently managing data subject rights requests; and
- (e) ensuring employees understand their data protection responsibilities.

12.3 What do you envision the privacy landscape will look like in five years?

Better regulated with more up-to-date legislation.

 NORTH MACEDONIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in North Macedonia.

Privacy in North Macedonia is regulated by the Law on Personal Data Protection ('LPDP'), which aligns with the EU General Data Protection Regulation ('GDPR'). It sets guidelines for data collection, processing, and transfer, requiring explicit consent and ensuring data security.

The LDPA regulates the following topics:

- (a) The processing of personal data, the principles related to the processing of personal data;
- (b) The rights and obligations of the data subject;
- (c) The position of the controller and the processor of personal data;
- (d) The data transfer to EU and non-EU member countries;
- (e) The establishment, status and competencies of the personal data protection;
- (f) The special operations for the processing of personal data, the legal remedies and liabilities regarding the processing of personal data.

The Personal Data Protection Agency ('DZLP') oversees compliance and enforces penalties for violations.

1.2 What are the primary laws regulating privacy in North Macedonia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

In addition to the LDPA, which is *lex generalis*, the Consumer Protection Law is also relevant, as are other sector-specific laws regulating personal data, covering areas such as audio and audio-visual media services, e-commerce, medicines, tobacco etc.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In North Macedonia, self-regulation plays a supplementary role in privacy regulation, particularly in advertising practices. While the LPDP provides the legal framework, industry-specific self-regulatory bodies, such as the Association of Advertisers in Macedonia, may set additional guidelines for ethical advertising. These self-regulatory measures help ensure compliance with data protection principles, promote transparency, and foster trust in advertising practices, especially when it comes to personal data use. However, legal enforcement through the DZLP remains the primary mechanism for ensuring privacy protection.

1.4 How is privacy law enforced in North Macedonia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

In North Macedonia, privacy law is enforced through a combination of regulatory oversight, self-regulation, private actions, and other enforcement mechanisms. The DZLP plays a central role in overseeing and ensuring compliance with data protection laws, including the LPDP and related regulations. The DZLP is empowered to issue rulebooks, guidelines, conduct inspections, and impose fines or corrective actions in case of non-compliance.

The DZLP also has the authority to investigate complaints, conduct audits, and ensure that organizations comply with privacy requirements. It can issue administrative orders, including warnings, reprimands, and directives for companies to remedy violations. In cases of significant breaches, the DZLP can impose fines of up to 4% of annual turnover of the company.

Individuals whose personal data rights have been violated can take private legal actions against the organizations responsible for the breach. This includes filing lawsuits for damages resulting from unlawful data processing or breaches. In some cases, individuals can seek judicial remedies through civil courts for violations of their privacy rights.

In addition, the Macedonian legal system also allows for actions through the courts if individuals or organizations are dissatisfied with the DZLP's decisions or seek further legal remedies. Moreover, companies must ensure compliance with international data protection standards, such as the EU GDPR, for cross-border data transfers, which might involve cooperation between the DZLP and other EU data protection authorities.

In conclusion, privacy law enforcement in North Macedonia relies heavily on the DZLP's regulatory oversight, with supplementary roles for self-regulation, private actions by individuals, and broader judicial mechanisms for ensuring compliance.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in North Macedonia?

Privacy law in North Macedonia applies to all companies that have their headquarters within the territory of North Macedonia and process personal data as controllers or processors in the course of activities conducted in North Macedonia, regardless of whether the processing itself takes place within the country.

Additionally, privacy law applies to companies that do not have their headquarters in North Macedonia but process personal data as controllers or processors, if the processing relates to:

- (a) offering goods or services to data subjects in North Macedonia, regardless of whether payment is required for such goods or services; or
- (b) monitoring the activities of data subjects, if those activities take place in North Macedonia.

2.2 Does privacy law in North Macedonia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the LPDP does apply to foreign companies that process personal data of individuals located in North Macedonia. Foreign data controllers or data processors are required to comply with the law when processing personal data related to North Macedonian data subjects. Moreover, foreign entities are obligated to appoint an authorized representative in North Macedonia, unless the processing:

- (a) is periodical;
- (b) does not involve the processing of special categories of personal data; and
- (c) is not expected to cause a risk to the rights and freedoms of natural persons.

When these exceptions do not apply, foreign companies must appoint a local representative in North Macedonia. This ensures that the foreign company has a contact point in the country to facilitate compliance and enforcement of the data protection regulations.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in North Macedonia?

Pursuant to the LPDP, 'personal data' means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as the first and last name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The LPDP defines sensitive data as 'special categories of personal data', including information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health data, and data related to a person's sex life or sexual orientation.

As a general rule, processing of such data is prohibited, except under specific conditions, such as explicit consent, legal obligations in employment and social security, protection of vital interests, legitimate activities of non-profit entities, public health, or scientific research. Processing must always comply with proportionality, necessity, and adequate safeguards to protect fundamental rights.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The key distinction in the LPDP is between data that can be used to directly identify an individual and data that cannot:

- (a) Anonymized data is not considered to be personal data because it has been altered in such a way that it cannot be used to identify individuals (even by the data controller). This means that data falls outside the scope of data protection regulations once it is truly anonymized, as it no longer qualifies as personal data.
- (b) Pseudonymized data, on the other hand, remains personal data because it still has the potential to be re-identified (for example, by using additional information). Pseudonymized data is subject to the same data protection requirements as other personal data under the LPDP.

It is important to ensure that pseudonymization or de-identification processes are robust and do not allow for re-identification, or else the data will continue to be treated as personal data subject to privacy protection regulations.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies processing personal data must adhere to key privacy principles, including:

- (a) **Lawfulness, fairness, and transparency:** Personal data must be processed in accordance with applicable laws, in a fair manner, and with transparency toward the data subject.
- (b) **Purpose limitation:** Data collection should be for specific, explicit, and legitimate purposes, and further processing must not be incompatible with those purposes.

- (c) **Data minimization:** Only data that is adequate, relevant, and necessary for the intended purpose should be processed.
- (d) **Accuracy:** Personal data must be accurate and kept up to date where necessary. Inaccurate data should be corrected or deleted without delay.
- (e) **Storage limitation:** Personal data should not be retained longer than necessary for the purposes for which it was collected.
- (f) **Integrity and confidentiality:** Appropriate security measures must be in place to protect personal data from unauthorized processing, accidental loss, destruction, or damage.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

- (a) **Data controllers** are entities that determine the purposes and means of processing personal data. They bear responsibility for ensuring compliance with the key privacy principles (for which see question 4.1). Controllers determine which personal data will be collected, the duration of its retention, and whether it will be shared with third parties.
- (b) **Data processors** are entities that process personal data on behalf of a controller. Their responsibilities include:
 - (i) Processing personal data strictly according to documented instructions from the controller;
 - (ii) Ensuring that individuals authorized to handle data are bound by confidentiality obligations;
 - (iii) Implementing technical and organizational measures to maintain data security;
 - (iv) Engaging another processor only with prior authorization from the controller;
 - (v) Assisting the controller in fulfilling obligations related to data subjects' rights and notifications of data breaches;
 - (vi) Either deleting or returning all personal data to the controller once the processing activities have concluded; and
 - (vii) Providing the controller with all necessary information to demonstrate compliance and facilitating audits when required.

These obligations are formalized through a contract or other legally binding act between the controller and processor, in accordance with the LPDP.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

In North Macedonia, the processing of personal data must adhere to a lawful basis, ensuring that individuals' rights and freedoms are safeguarded. Similar to the EU GDPR, the country's data protection framework requires that companies and organizations justify their processing activities based on specific legal grounds.

Consent remains one of the primary bases, requiring individuals to give clear and explicit authorization for their data to be processed for a particular purpose. Beyond consent, processing is also permitted when necessary for the performance of a contract, compliance with legal obligations, or the protection of an individual's vital interests. Additionally, public authorities may process data when carrying out tasks in the public interest or exercising official authority.

A significant aspect of North Macedonia's data protection regime is the recognition of legitimate interests as a lawful basis for processing. This allows organizations to handle personal data in pursuit of their own or a third party's legitimate objectives—provided that such interests do not override the fundamental rights and freedoms of data subjects.

By ensuring that data processing always relies on a clearly defined legal basis, the framework aims to strike a balance between regulatory compliance, business interests, and the fundamental right to privacy.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

In North Macedonia, when companies process personal data for advertising purposes, they must ensure transparency in their privacy notices. These notices should clearly identify the data controller, the purpose of processing (especially for advertising), and the legal basis for processing, such as consent or legitimate interest. Individuals must be informed of their rights, including the ability to access, correct, and withdraw consent for their data.

However, it's important to note a distinction when processing data for business-to-business (B2B) advertising. In B2B cases, the privacy notice may not always apply to personal data related to the business contacts of companies. In these instances, the requirements may be less stringent, as the data processed is related to professional rather than personal information.

In all cases, companies must also disclose the data retention period, any third-party data sharing, international data transfers, and automated decision-making, including profiling. By providing these details, companies ensure compliance with privacy laws and maintain trust with both individuals and business partners.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

In accordance with the Consumer Protection Law, certain practices are prohibited and deemed unfair and aggressive, irrespective of the factual circumstances. In this regard, an 'unfair and aggressive practice' includes the case where a company persistently and without consent contacts consumers via telephone, fax, email, or other means of remote communication, except when justified under applicable regulations for fulfilling contractual obligations. A consumer may exercise the protection of their rights through submitting a consumer complaint to the company, initiating a consumer dispute in civil proceedings, or resolving consumer disputes out of court.

A company, or a company providing a public service, is obliged to allow the consumer to submit a complaint in cases where their rights under this law or a contract have been violated. Furthermore, the company must process the consumer complaint in accordance with the law, irrespective of whether the complaint is explicitly designated as such. This is without prejudice to the provisions on distance contracts, the LPDP, and regulations on privacy protection in electronic communications.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

In North Macedonia, the LPDP, aligned with the EU's GDPR, governs advertising activities that involve the processing of personal data. Under the LPDP, companies must obtain explicit consent from individuals before processing their personal data for direct marketing purposes. This consent is mandatory for business-to-consumer (B2C) marketing, ensuring that individuals are aware of and agree to the use of their data for promotional activities.

For electronic marketing methods, such as emails, text messages, or online advertisements, the LPDP requires that companies obtain explicit consent from data subjects prior to processing their personal data. Additionally, individuals have the right to object to the processing of their personal data for direct marketing purposes, providing them with an opt-out option. As mentioned above, it's important to note that business-to-business (B2B) marketing falls outside the scope of the LPDP. Therefore, prior consent is not required for B2B marketing activities under this law.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

North Macedonia's privacy law requires that any vendor or third party involved in advertising—such as advertising agencies, DSPs, SSPs, or data providers—adhere to strict data protection principles. This means obtaining explicit consent for the processing of personal data, ensuring transparency, and applying adequate security measures as mandated by the LPDP. Additionally, when consumer data is used in advertising, the Consumer Protection Law also comes into play to ensure fair and transparent practices.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When sharing personal data with vendors or receiving data from them, companies must establish clear data processing agreements. These contracts should specify the purposes of processing, impose confidentiality and security obligations, set out breach notification procedures, and grant audit rights to ensure compliance with LPDP principles.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

In North Macedonia, companies are mandated to conduct a Personal Data Protection Impact Assessment ('PDPIA') before initiating any data processing activities that could pose a high risk to individuals' rights and freedoms. This requirement aligns with the LPDP, which emphasizes the necessity of assessing potential impacts when implementing new technologies or processing methods.

The PDPIA process involves:

- (a) Describing the intended data processing operations;
- (b) Evaluating their necessity and proportionality;
- (c) Identifying and managing risks to individuals' rights and freedoms; and
- (d) Implementing measures to mitigate identified risks.

It's crucial that this assessment is performed prior to the commencement of data processing, ensuring compliance from the outset. This proactive approach is part of the broader principle of accountability, requiring controllers to apply appropriate technical and organizational measures to demonstrate adherence to data protection regulations.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Law on personal data processing defines 'direct marketing' as any type of communication taking place by any means with the purpose of imparting advertising, marketing or publicity materials targeting directly a specific data subject, as well as personal data processing which includes profiling to the extent that it is related to this type of communication.

Personal data processing for the purposes of direct marketing is allowed upon prior explicit consent given by the data subject. Individuals must be clearly informed by the controller prior to giving their consent:

- (a) why their data are being collected,
- (b) how their data will be used,
- (c) if the data are being transferred and where,
- (d) regarding their right to object to the processing or to withdraw their consent etc.

An easy opt-out option must be provided. Further, the data subject has the right to object at any time to the processing of their personal data for direct marketing, in which case the controller must stop with its processing.

As to consumer protection in relation with direct marketing, please see question 5.2.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The Rulebook on the Security of Personal Data Processing (122/2020) briefly addresses the use of cookies in safeguarding data on a data controller's webpage. Specifically, when using non-essential cookies, the data controller must obtain prior consent from the internet user after providing appropriate notice, before the cookie is deposited.

In North Macedonia the use of cookies (or any other method of storing information on or gaining access to information already stored on the subscriber's or user's terminal equipment) is regulated in the Law on Electronic Communications. This is only permitted if the subscriber or user concerned has given consent, after being provided with clear and comprehensive information regarding the data collection, its processing, the purpose thereof etc in accordance with personal data protection regulations. Only cookies that are technically necessary to enable communication between the user's terminal equipment and the website they are visiting or to provide the website's service at the user's request are excluded from this rule for requesting and granting consent.

Each website must have a cookie policy.

On the other hand, the LPDP regulates what represents personal data, how can they be legally processed, who can process personal data, the rights of the data subject, controller's and processor's obligations, and supervision.

7.3 How are loyalty programs and promotions regulated under privacy law?

Promotions are considered as direct marketing.

In order to collect and process personal data for loyalty programs, consent of the data subject is required. The data subject must be informed of what personal data are collected and for what purpose, their rights (such as the right to withdraw consent), the terms of the loyalty program, and other similar information.

7.4 How is social media and influencer marketing regulated under privacy law?

Currently, no specific laws in North Macedonia directly regulate influencers. However, there are ongoing developments in this area. The Director of the Agency for Audio and Audiovisual Media Services has publicly stated that a procedure is underway for drafting a Rulebook on influencers. This Rulebook is expected to address key issues, particularly advertising regulations, and is anticipated to be adopted this year (2025).

Based on public statements from the Director, the Rulebook will primarily aim to regulate influencers whose primary purpose is to inform, entertain, or educate and who create content for the general public, rather than for a specific, limited group. No further details are currently available. However, given the increasing presence and influence of social media personalities in the country, the adoption of this Rulebook is expected to address a significant legal gap. It is anticipated to strengthen the regulatory framework concerning influencer activities, particularly in relation to privacy laws and advertising practices.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

In North Macedonia, the LPDP governs all forms of advertising that involve the processing of personal data, including targeted advertising (such as behavioral or personalized advertising) and contextual advertising:

- (a) **Targeted advertising** involves collecting and analyzing user behavior to deliver personalized ads. This practice requires explicit consent from the individual before their data can be processed for such purposes. The law mandates that individuals have the right to object to the processing of their data for direct marketing purposes at any time. Upon such objection, the processing must cease immediately. If targeted advertising involves profiling (analyzing aspects of an individual's behavior, preferences, or interests), explicit consent for the profiling is also required. Failure to obtain this consent can result in fines of up to 2% of the company's total worldwide annual turnover from the preceding financial year.
- (b) **Contextual advertising** delivers ads based on the content of the webpage or the context in which the ad appears, rather than personal data. Since this method doesn't involve processing personal data, it generally falls outside the scope of personal data protection laws. Therefore, explicit consent from individuals is not required for contextual advertising.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific regulations on digital identity resolution and clean room technologies, therefore such practices must adhere to the general data protection framework outlined in the LPDP.

7.7 How is location-based advertising regulated under privacy law?

In North Macedonia, location-based advertising but falls under the general provisions of the LPDP, which aligns with the GDPR. This means that businesses must obtain explicit consent from individuals before processing their location data for advertising purposes. Additionally, data controllers must ensure transparency, purpose limitation, and security when handling such personal information.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific regulations governing data brokers; consequently, the general provisions on personal data protection will apply.

7.9 How is advertising to children and minors regulated under privacy law?

In North Macedonia, the advertising of products and services to minors is primarily governed by general consumer protection laws and specific provisions under the LPDP, as well as the Law on Audio-Visual Media Services:

- (a) **The Consumer Protection Law** prohibits advertising that targets minors in a way that could exploit their lack of experience, judgment, or capacity to understand the advertising message. Such practices are deemed aggressive trade practices that are always considered as unfair. The law protects children from being misled by commercial practices, particularly those that may harm their physical or mental development. It also bans advertisements that pressure minors into making purchasing decisions or induce them to exert undue influence on their parents or guardians.
- (b) **LPDP:** While this law does not specifically address advertising to minors, it protects minors' personal data. Advertisements targeted at minors often involve the collection of personal data (eg, via cookies or tracking technologies). In such cases, the collection of personal data from minors is subject to parental consent, as minors are generally considered to be unable to provide informed consent themselves.
- (c) **The Law on Audio-Visual Media Services** places restrictions on advertising content directed at minors, ensuring that advertisements do not contain content that could harm minors' well-being. It also sets limits on the volume and frequency of advertisements shown during children's programming, ensuring that the amount of advertising aimed at minors is controlled.
- (d) **General advertising practices:** Any advertising directed at minors must not:
 - (i) Undermine their physical, mental, or moral development.
 - (ii) Encourage minors to engage in harmful behaviors (eg, unhealthy eating, gambling, or unsafe use of products).
 - (iii) Mislead minors into making decisions that are not in their best interests.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

When it comes to automated decision-making and profiling, which may have legal effects or significantly affect individuals, such decisions are prohibited unless certain conditions are met. These conditions include the necessity of the decision for contract performance, legal authorization, or explicit consent from the individual.

7.11 Are there other specific advertising practices that you wish to discuss?

On March 13, 2024, North Macedonia's parliament lifted a six-year ban on state-funded advertisements in private media by amending the Law on Audio and Audiovisual Media Services. The changes allow the government and municipalities to allocate up to 0.1% of collected taxes for media campaigns, with oversight from a commission including ruling and opposition representatives. Journalist unions and media organizations warn this move could reintroduce political influence, advocating instead for a Media Pluralism Fund to support independent journalism.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The DZLP assesses whether a third country or organization ensures an adequate level of protection. This determination is based on whether the third country offers protections substantially equivalent to those in North Macedonia and provides effective rights and remedies for data subjects. The DZLP may approve, amend, or revoke adequacy decisions.

Transfers to EU/EEA countries, or those deemed adequate by the European Commission (eg, Andorra, Canada, Israel, New Zealand, Switzerland, and the US for Privacy Shield-compliant companies), do not require DZLP approval. However, controllers/processors must notify the DZLP at least 15 days in advance.

In the absence of an adequacy decision, data transfers are permitted if appropriate safeguards are in place, such as:

- (a) Standard Contractual Clauses ('SCC's): ie, pre-approved contractual terms ensuring data protection obligations between the exporter and importer;
- (b) Binding Corporate Rules ('BCR's): ie, internal, legally binding data protection policies within multinational groups, approved by the DZLP;
- (c) Approved Codes of Conduct: ie, sector-specific guidelines ensuring compliance with data protection standards.
- (d) Certification mechanisms: ie, independent verification of compliance with data protection requirements; and
- (e) Legally binding public agreements: ie, agreements between public authorities with enforceable data subject rights. In specific cases, transfers without safeguards may be allowed under explicit consent, legal claims, or public interest considerations.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

N/A

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in North Macedonia? Are there minimum standards? Does this differ by sector or size of the entity?

In North Macedonia, data security is regulated by the LPDP, which aligns with the EU's GDPR. The law requires data controllers and processors to implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of personal data. The DZLP oversees compliance with these requirements.

A key principle under the LPDP is the implementation of risk-based security measures, meaning that organizations must assess potential risks associated with data processing and apply appropriate safeguards. While the law does not impose specific security standards based on sector or company size, all entities handling personal data must implement measures proportional to the nature, scope, and purposes of data processing.

To ensure compliance, organizations must apply a combination of technical and organizational measures, including:

- (a) **Pseudonymization and encryption:** The LPDP encourages the use of pseudonymization and encryption to enhance data security, reducing the risk of exposure in case of unauthorized access;
- (b) **Access control and authentication:** Implementing role-based access, multi-factor authentication, and logging mechanisms to prevent unauthorized data access;
- (c) **Data minimization and storage limitation:** Ensuring that only necessary personal data is collected, stored for a limited period, and securely deleted when no longer required;
- (d) **Incident response and breach notification:** Organizations must establish protocols for detecting, managing, and reporting data breaches to the DZLP within 72 hours, when applicable; and
- (e) **Regular security audits and risk assessments:** Conducting periodic assessments to identify vulnerabilities and ensure ongoing compliance.

9.2 How are personal data breaches regulated in North Macedonia? What are the requirements for notification and response?

Personal data breaches are governed by the LPDP, which aligns with international data protection standards. The DZLP serves as the supervisory authority overseeing compliance with these regulations:

- (a) **Notification requirements**
 - (i) to the DZLP: Data controllers and processors are mandated to notify the PDPA of personal data breaches without undue delay. This notification should include details such as the nature of the breach, the categories of data affected, and the measures taken to address the breach.
 - (ii) to Data Subjects: If a breach is likely to result in a high risk to the rights and freedoms of individuals, data controllers must inform the affected data subjects promptly. This communication should describe the breach's nature, potential consequences, and measures taken to mitigate potential adverse effects.
- (b) **Response obligations:** Upon discovering a personal data breach, data controllers are required to:

- (i) Assess the breach: Evaluate the breach's impact, including the type of data involved and the potential harm to individuals.
- (ii) Contain and mitigate: Implement measures to secure the data and prevent further unauthorized access or loss.
- (iii) Document the incident: Maintain a detailed record of the breach, including its circumstances, effects, and remedial actions taken.
- (iv) Cooperate with the DZLP: Provide the DZLP with all necessary information regarding the breach and collaborate during any investigations.

Failure to comply with these notification and response requirements can result in administrative sanctions, including fines, as enforced by the DZLP. Therefore, it is essential for organizations operating in North Macedonia to establish robust data breach response protocols to ensure compliance and protect individuals' personal data.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

In North Macedonia, non-compliance with the LPDP can lead to administrative fines, corrective measures, and, in some cases, criminal liability. The DZLP oversees compliance and has the authority to impose sanctions based on the nature and severity of the violation.

Financial penalties under the LPDP can be significant, with companies facing fines ranging from €1,000 to €10,000, and in more severe cases, up to 4% of their total annual revenue. Individuals responsible for violations, such as managers or employees handling personal data, may also be fined between €500 and €1,500. Serious infringements include processing personal data without a valid legal basis, failing to implement adequate security measures, non-compliance with data subject rights, unauthorized data transfers, and failure to report data breaches within the required 72-hour period.

Beyond monetary fines, the DZLP can order companies to halt unlawful data processing, implement necessary security measures, or restrict certain data activities. In cases of intentional misuse or serious breaches, criminal sanctions under the Criminal Code may apply, including potential imprisonment for individuals involved.

Given the increasing enforcement of data protection rules, organizations must prioritize compliance by adopting robust security measures, conducting regular audits, and ensuring employees are adequately trained in data protection obligations.

10.2 Do consumers have a private right of action? What remedies are available to them?

The Consumer Protection Law considers certain marketing practices, such as unsolicited emails or forced marketing, to be unfair trade practices. These types of practices are deemed unlawful when businesses engage in aggressive or misleading marketing tactics, especially when personal data is involved. For example, consumers may receive unsolicited emails or messages promoting products without their prior consent, or they may be subject to pressure to purchase goods under misleading conditions.

In response to such unfair trade practices, the Consumer Protection Law provides several remedies for consumers:

- (a) **Right to object:** Consumers have the right to object to unsolicited marketing or any marketing activities that they consider deceptive or aggressive. This includes the right to withdraw consent if they had previously agreed to receive such marketing communications, especially in cases involving personal data;
- (b) **Right to cessation of unfair practices:** Consumers can demand that the business immediately stops the unlawful practice, eg, discontinues unsolicited email marketing. This is a key protection for consumers against intrusive practices;
- (c) **Compensation for harm:** If consumers suffer harm due to unfair trade practices, including distress or financial damage caused by unsolicited communications or forced marketing, they may be entitled to compensation. This can be pursued through complaints or legal action against the business; and
- (d) **Filing complaints:** Consumers can report unfair trade practices to the State Market Inspectorate or relevant authorities tasked with overseeing consumer protection. These bodies have the power to investigate complaints, issue warnings, and impose penalties on companies engaging in unlawful marketing practices.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

According to the annual report of the DZLP, the primary focus in 2023 was raising public awareness of the importance of personal data protection among individuals, data protection officers, controllers, and processors, as well as enhancing individuals' understanding of their rights and the means available for their enforcement.

The agency placed particular emphasis on conducting investigative mandates and supervisory activities, resulting in the submission of six requests for initiating misdemeanor proceedings, based on which fines totaling 1,554,881 denars (approx €25,250) were imposed.

The main priority remains the implementation of the LPDP, ensuring the continuous compliance of controllers and processors while strengthening the agency's independent status and aligning its framework with EU legislation.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in North Macedonia?

There are no cultural considerations that impact privacy law enforcement in North Macedonia.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Companies operating in North Macedonia should keep a close eye on several emerging issues and legal challenges related to privacy law and data protection. Key 'hot topics' include:

- (a) **Extra-territorial applicability and local representation:** As the LPDP increasingly aligns with the EU GDPR, companies—especially those based outside North Macedonia—must monitor evolving requirements around the extraterritorial scope and the need to appoint local representatives;

- (b) **Cross-border data transfers:** With ongoing discussions about adequacy decisions and safeguards such as SCCs and BCRs, businesses should watch for any changes that might affect how they legally transfer personal data outside North Macedonia;
- (c) **Consent and transparency requirements:** Enhanced consent mechanisms for processing personal data—especially in digital environments, including the use of cookies and tracking technologies—remain a focal point. Companies should be alert to any new guidance or stricter enforcement practices regarding how consent is obtained and documented;
- (d) **Enforcement trends and penalties:** Given the potential for significant fines (up to 4% of annual turnover in severe cases) and increased scrutiny by the DZLP, companies should monitor enforcement practices and adjust their data protection strategies accordingly; and
- (e) **Emerging technologies:** As technologies like artificial intelligence and biometric data processing become more prevalent, regulatory bodies may introduce new requirements or clarify existing ones. Keeping abreast of these changes will be crucial for compliance.

In summary, companies should continuously review their data protection policies in light of these evolving issues, ensure robust consent and security measures are in place, and consider the implications of any cross-border data transfers within this dynamic legal landscape.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The key challenge in the field of personal data protection remains keeping up with evolving legal frameworks, as new laws are continuously being adopted and existing ones amended. Additionally, the rapid advancement of technology and artificial intelligence is expected to necessitate further regulatory adaptations in the foreseeable future. Regarding most recent developments, see question 12.1, which outlines the adoption of the new Rulebook on Security of Personal Data and its implications.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The most recent change is the new Rulebook on Security of Personal Data Processing, which will enter into force on July 1, 2025, replacing the existing Rulebook. The new Rulebook introduces several key changes and requirements, including:

- (a) **Information system implementation and documentation:** Data controllers are required to prepare and maintain comprehensive documentation for all information systems that process personal data. This documentation must include:
 - (i) a clear definition of the purposes for which personal data is processed;
 - (ii) a detailed mapping and documentation of each personal data processing activity;
 - (iii) the technical specifications of the system.
- (b) **Information system maintenance and updates:** The Rulebook mandates an ongoing review and timely updates of information systems, with particular emphasis on:
 - (i) the technical and organizational measures in place to ensure data security;
 - (ii) ensuring that any third parties responsible for system maintenance comply with the Rulebook's requirements.

- (c) **International data transfers:** Transfers of personal data to third countries are permitted only when such transfers comply with North Macedonian data protection regulations. This provision emphasizes the necessity for thorough assessments of all international data transfers and the implementation of appropriate safeguards.

These changes are designed to enhance the overall security framework for personal data processing and to ensure that North Macedonia's regulatory environment remains aligned with international standards.

Overall, the Rulebook requires organizations to adopt a risk-based approach to data security, mandating comprehensive risk assessments that categorize data processing activities based on potential harm and likelihood of breaches. Companies must implement technical and organizational safeguards proportional to the identified risks, ensuring that higher-risk processes receive more robust protection. Furthermore, the rulebook enhances oversight by establishing clearer procedures for regular inspections and stricter reporting requirements for data breaches.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

It may be anticipated that challenges will arise that derive from the coming into effect of the new Rulebook on Security of Personal Data Processing (see question 12.1). A key challenge will be proactive risk management. Companies are required to conduct regular and documented risk assessments to address potential data security threats, such as unauthorized access and data loss. They must also implement technical and organizational measures to mitigate these risks. The Rulebook includes annexes with guidelines on risk assessment methodology and required security measures. Additionally, companies must document forensic investigations related to data breaches, including investigation results. Non-compliance can lead to fines of up to 4% of annual income, emphasizing the importance of adherence to these new obligations.

12.3 What do you envision the privacy landscape will look like in five years?

In the next five years, the privacy landscape in North Macedonia is expected to continue evolving in line with EU regulations. The focus will likely remain on strengthening enforcement mechanisms, ensuring the continuous compliance of data controllers and processors, and enhancing public awareness of data protection rights.

Additionally, the rapid advancement of artificial intelligence and digital technologies is expected to drive regulatory updates, potentially requiring new legislative frameworks to address emerging privacy risks. Looking ahead, North Macedonia is likely to further align with EU legislative developments, such as potential new AI regulations and stricter cross-border data transfer rules, ensuring a more harmonized and adaptive privacy framework.

 NORWAY 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Norway.

Privacy is a constitutional right in Norway. The constitutional right to privacy is similar to that in the European Convention on Human Rights ('ECHR') article 8, which is also included in Norwegian law. 'Privacy' covers more than solely personal data; covering aspects such as a prohibition on damaging others' reputation.

The right to privacy must be balanced against freedom of expression. The courts generally attach great importance to freedom of expression. This was recently underlined in a case concerning a website containing reviews of medical practitioners (this case mainly concerned legitimate interests under the EU General Data Protection Regulation ('GDPR')) .

For personal data, the Personal Data Act applies. The Personal Data Act implements the GDPR in Norway. Norway is not an EU Member State, thus the GDPR does not automatically apply, but Norway is obligated to implement the GDPR through the European Economic Area Agreement. There is a presumption of conformity of Norwegian domestic law with EU law. Norwegian national courts are under an obligation to interpret national provisions in such a way to avoid conflict with EU law to the maximum extent possible.

The Norwegian Personal Data Act has several provisions in addition to the GDPR. Some of these provisions will be discussed below.

For communications, the European Electronic Communications Code is also substantially incorporated into Norwegian legislation, being written into in the new Electronic Communications Act, which came into effect on January 1, 2025.

1.2 What are the primary laws regulating privacy in Norway? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

As mentioned above, the main framework consists of the Constitution, the GDPR, the Personal Data Act and the ePrivacy rules. Norway also has sector-specific national codes and regulations:

- (a) **Electronic marketing:** The Marketing Act requires consent for marketing with electronic methods of communication in the course of trade, such as email and automated calls.
As an exception to this, consent is not necessary if there is an existing customer relationship, where the business has received the customer's electronic address in connection with a sale. A one-time purchase, for instance of an inexpensive, disposable item, will not, as a rule, be seen as establishing an customer relationship between seller and buyer. However, with purchases of capital goods, such as a car, or washing machine, it is to be expected that the seller continues contact with the customer. Again, where repeated purchases of inexpensive, disposable items are made within a short period of time, a customer relationship may considered to exist.
- (b) **Employment:** The question of access to emails and other electronically stored material of an employee is regulated in a specific Regulation. An employer can only access current or former employees' emails or private files in two cases:
 - (i) when it is necessary to safeguard the operation of the business or other legitimate interests of the business; and

(ii) on suspicion of gross breach of the employee's duties.

Automatic forwarding of emails is considered a continuous monitoring of the employee's use of electronic equipment and is not allowed.

Monitoring of an employee's use of electronic equipment is prohibited and is only allowed if the purpose is to administer the company's computer network or detect or solve security breaches in the network and the monitoring measure is necessary for these purposes.

There are also important provisions in the Working Environment Act which concern privacy. These include surveillance of employees and specific rules for control measures aimed at employees.

- (c) **Security in public bodies:** See the European Union chapter. In addition, detailed security requirements are often found in regulations and widely-used standard agreements required by the government.

The Norwegian Freedom of Information Act aims to ensure transparency in the public sector by granting the general public access to official documents held by public authorities. However, this right is balanced against the protection of personal data, as regulated primarily by the Personal Data Act and the GDPR. When documents contain personal information, public authorities must assess whether the information can be disclosed without violating privacy rights. In practice, this often leads to redaction of names, identification numbers, or sensitive personal details before documents are made public. Thus, while the Act promotes openness, it is interpreted and applied in a way that safeguards individuals' privacy in accordance with data protection laws.

- (d) **Health:** In the health sector, privacy is heavily enacted.

This list is not exhaustive, there are several more special Norwegian privacy rules.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulatory bodies do not have enforcement powers equivalent to the data protection authority, Datatilsynet, in this field. Datatilsynet has repeatedly emphasized that self-regulation cannot replace legal obligations—especially regarding explicit consent, data subject rights, and processing of sensitive data.

However, there are examples of self-regulatory guidelines for digital marketing. They are especially useful in promoting best practices and ensuring consistency across the advertising sector. Self-regulation often sets practical standards for how to obtain and manage user consent, in compliance with GDPR. These frameworks emphasize notice, consent, and opt-out mechanisms for interest-based advertising. For example, in the use of cookies and tracking technologies, the industry has developed cookie banners and consent management platforms (CMPs) based on self-regulatory templates. However, self-regulatory guidelines must be auditable and align with the GDPR's consent requirements (freely given, specific, informed, and unambiguous), which are enforced by Datatilsynet.

1.4 How is privacy law enforced in Norway? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

There are several supervisory authorities which enforce privacy rules:

- (a) The Norwegian data protection authority, Datatilsynet, enforces the Norwegian Personal Data Act which implements the GDPR;

- (b) The supervisory authority under the cookie provision in the Electronic Communications Act is shared between Datatilsynet and the Norwegian Communications Authority, Nkom:
 - (i) Nkom is responsible for assessing whether a technical solution falls within the scope of the provision and whether the exceptions from the requirement of information and consent are fulfilled, and
 - (ii) Datatilsynet is responsible for assessing whether sufficient information is provided and whether the consent meets the requirements set out in the GDPR;
- (c) the Consumer Authority is the relevant authority for breaches of the Marketing Act. Decisions by the Consumer Authority can be contested in court. Persons and entities can bring claims for breaches of the Marketing Act to court. In Norwegian court practice, such cases are typically brought to prevent a breach, combined with a claim for damages.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Norway?

See the European Union chapter. The concepts of ‘controller’ and ‘processor’ are defined and interpreted in accordance with the GDPR in Norway.

2.2 Does privacy law in Norway apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

See the European Union chapter.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Norway?

See the European Union chapter.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

While not formally considered as special categories of personal data (in terms of the GDPR), processing of unambiguous identifiers, such as personal identity numbers, is prohibited. Unambiguous identifiers may only be processed if there is objective need for secure identification.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter. In Norway, Datatilsynet currently seems to be specially interested in security and privacy by design and default.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter. The concepts of ‘controllers’ and ‘processors’ are the same.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter.

The Norwegian Personal Data Act has some exceptions to the data subject’s right to access. These provisions are mainly applicable for public bodies; in rare cases exceptions they may also be applicable for private bodies.

To ensure freedom of expression, the Norwegian Personal Data Act also has exceptions to data subjects’ rights.

In the Norwegian Copyright Act, there are rules requiring consent before using pictures of persons who are photographed, although there are some exceptions, mainly to ensure freedom of expression and freedom of business.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

According to the Marketing Act electronic marketing to natural persons is prohibited without their prior consent, and those that receive marketing based on consent must be given a simple and free way to opt out of such communications, and must be informed of this option each time they receive marketing material. When marketing is sent via email, for example, there should be an option to say ‘no thanks’ using a link included in each individual email. When marketing is sent via SMS, there should be an option to respond via SMS as well as through the trader’s website.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter and question 8.2.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

As mentioned in question 1.2, the Marketing Act requires consent for most electronic marketing communication carried out by enterprises, such as email and automated calls.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

In addition to the GDPR, the European Electronic Communications Code is also substantially incorporated into Norwegian legislation, in the new Electronic Communications Act, which came into effect on January 1, 2025.

Consent is explicitly required for cookies. The consent requirement in the Electronic Communications Code is in line with the requirement in the GDPR.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

Norway has decided that data subjects who are 13 years or older can consent to information society services.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

Norway has decided that data subjects who are 13 years or older can consent to information society services.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Norway? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

In the Working Environment Act, and in the health, energy and finance sectors, there are more specific codes, regulations and guidelines on data security.

The Norwegian Security Code is applicable to those selling to public bodies, for deliveries which may access classified information or critical objects or infrastructure. As systems are interconnected, this Code applies in many cases.

Additional framework codes on data security are currently being assessed by the Ministry of Justice.

The Acts and codes also apply to non-personal data.

Datatilsynet has an ombudsman role for issues relating to personal data, namely to provide advice and information. This is done, amongst others, by means of guidelines and information published on its website.

9.2 How are personal data breaches regulated in Norway? What are the requirements for notification and response?

See the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter.

In addition, there are some rules which are specific to Norway. If more than five years have elapsed after a breach of the law, Datatilsynet may not fine the controller or processor, unless it finds that there is an ongoing case.

Also, in addition to fines, Datatilsynet may impose liquidated damages for every day the controller or processor fails to act as ordered by Datatilsynet.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter.

Individuals can file a complaint anonymously to Datatilsynet. Individuals can also claim damages—even if the individual has not suffered any economic loss.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The enforcers are quite active. Recently, Datatilsynet conducted inspections of several websites' use of tracking pixels. It was found that all of the websites inspected unlawfully shared visitors' personal data with third parties, and, in several cases, the data included sensitive information. In one case, following the inspection, Datatilsynet imposed an administrative fine of NOK 250,000 (approx €21,860).

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Norway?

Norwegian culture is privacy-oriented in comparison to several other cultures. Norway has a tradition of strict privacy rules.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Datatilsynet continues to file legal complaints against Ad-tech companies for breach of the GDPR. In 2023, it won a court case against Meta. In addition, Datatilsynet states that they assess several current Ad-tech solutions to be threats to privacy and, in a broader sense, society.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Fake surveillance gear not actually processing data is subject to privacy law. Thus, the scope of the Norwegian Personal Data Act is wider than in other countries. One of the justifications for this rule may be along the lines of such surveillance being like Bentham's 'Panopticon': if the data subject's behavior is affected because of a false impression that they are being observed, this still represents an infringement of privacy. In these cases, even giving the impression of processing data requires privacy law compliance.

Also note the prohibition on processing of unambiguous identifiers discussed in question 3.2.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

- (a) The authorities are concerned and interested in the use of AI and its impact on privacy;
- (b) The authorities have focused more on security breaches and inspections, including inspection at government and large enterprises; and
- (c) Data subjects continue to be aware of their privacy rights.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Privacy will shift from being largely compliance-driven to becoming a core component of digital trust and corporate reputation. Organizations that treat privacy as a strategic priority—integrating it by design into products and services—will have a competitive advantage.

12.3 What do you envision the privacy landscape will look like in five years?

In five years' time, we envision a privacy landscape that is both more regulated and more complex, shaped by evolving technologies, geopolitical dynamics, and growing public awareness. We will likely see continued expansion and harmonization of data protection laws, with jurisdictions outside the European Union increasingly adopting GDPR-like frameworks.

We may also see increased user demand for transparency and control over personal data, possibly supported by new privacy-enhancing technologies and standards.

The tension between innovation and regulation will persist. The challenge is, and continues to be, to strike a balance between enabling technological progress and protecting fundamental rights.

PARAGUAY

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Paraguay.

In Paraguay, privacy law is regulated by means of several pieces of legislation, beginning with Paraguay's Constitution, which, under the title 'with respect to the right of intimacy', establishes that: 'personal and family intimacy, as well as the respect of private life, is inviolable. The conduct or behavior of people, if this does not affect the public order established by the law, or third parties' rights, is exempted from public authority. The right to the protection of intimacy, dignity and the private image of people is guaranteed'.

There are several other regulations, criminal, administrative and civil, related to the rights to privacy and intimacy, most important of which is the Personal Credit Data Protection Law (Law No 6534/20) which was passed by Congress and approved by the Executive Power in 2020. The objective of this Law is to guarantee the protection of credit data of everyone, regardless of the person's nationality, place of residence or address; it also regulates the collection and access to credit information data and the establishment, organization, functioning, rights and termination of corporations whose main activity is the obtaining and provision/communication of credit information.

1.2 What are the primary laws regulating privacy in Paraguay? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

As stated in question 1.1, the most important laws regulating privacy in Paraguay are the Constitution and the Personal Credit Data Protection Law. In addition:

- (a) The Criminal Code punishes conduct (felonies, in most cases) including:
 - (i) the violation of the intimacy of a person, the infringement of the rights to private communication and the rights to one own image;
 - (ii) the infringement of a person's confidentiality or right to keep their communications confidential, especially those via telephone or instant messaging; and
 - (iii) the violation of a person's private correspondence and the revelation of a private secret.

Under a different section, the Criminal Code sets out a series of conducts (felonies) that may affect a person's honor, including slander, defamation and insult;
- (b) The Civil Code regulates rights associated with a person's name and establishes that anyone injured by means of the unlawful use of their name has a right of action to stop such unlawful use and to demand damages;
- (c) Copyright law provides that a person's image may not be traded without the person's consent, unless the use is related to scientific, educational or cultural objectives or to facts or deeds of public interest that took place in public;
- (d) Trademark law protects people against the registration of their name;
- (e) The Law on Electronic Trade (Law No 4868/13) establishes that providers of electronic services (whether providing goods and services via electronic means, or providing electronic links, etc) may, under no circumstances, violate the moral and the protection of individuals who are consumers or users and the protection of personal data or personal or family intimacy rights and the confidentiality of bank accounts or registries; and

- (f) Consumer Protection Law (Law No 1334/98) regulates advertising, although it does not have any provision that refers explicitly to the rights of privacy. However, the violation/infringement of the rights of privacy as per the terms of the regulations mentioned above could be considered abusive publicity according to the Consumer Protection Law.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays a key role in privacy regulation.

The Advertising Self-Regulation Code is mandatory for all members of CERNECO, an association of advertisers, advertising agencies and the media. The authority in charge of interpreting and applying the provisions of the Code is CONAR, whose objective is the self-regulation of advertising, proposing through its recommendations that advertising messages be framed within the principles of legality, honesty, decency and truthfulness.

CONAR is responsible for studying and resolving all cases of alleged non-compliance with the provisions of the Code and the legal regulations in force, being able to act on its own initiative or in response to complaints received, regardless of their origin.

Where privacy is concerned, the Self-Regulation Code determines that advertising must be carried out with a sense of social responsibility and must respect the dignity of individuals, their privacy, family, social interests, as well as the authorities, public and private institutions and the country's symbols.

The Code contains a section on privacy protection, in which it determines that the use in advertising of images, photos, and quotations of and references to living persons, firms or institutions is prohibited unless express authorizations have been previously obtained; also, advertising that reveals a lack of respect for the dignity of the person or institution or that does not respect private property is not allowed.

Under the same section, the Code prohibits publicity containing images disrespectful of the good name and fame left by deceased people.

However, these rules do not apply to:

- (a) photographs of large groups or crowds, in which individuals may be recognized, but without involving them in a defamatory, offensive or humiliating context.
- (b) publicity for books, films, radio and television programs and similar activities, in which the people portrayed are authors or participants.

1.4 How is privacy law enforced in Paraguay? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy laws are enforced via different actions and before various courts/authorities:

- (a) There is a special constitutional institution, named 'amparo' or 'constitutional motion', by which any person who, as a result of an illegitimate act or omission of an authority or of an individual/corporation, considers himself gravely affected, or in imminent risk of being affected with respect to rights or guarantees foreseen by the Constitution or by Law, and, in view of the urgency of the case, cannot remediate the situation by ordinary means, may file a constitutional motion before a competent court in order to have the situation reversed. The procedure is brief, immediate and free-of-charge.

- (b) Lawsuits may be promoted before the civil courts or where applicable, before the criminal courts.
- (c) Individuals may also file a complaint before the Direction of User and Consumer Protection ('SEDECO') and/or the Paraguayan Central Bank, requesting the investigation of a data breach (especially when there is a breach in credit information data, as per the terms of the Personal Credit Data Protection Law) and the imposition of a fine or administrative punishment.
- (d) In the private sector, a complaint for breach of any of the norms of the Self-Regulation Code may be brought before the CONAR by the government and governmental institutions; consumer associations, associations and/or guilds that have a direct interest in the complaint; advertisers; the media; advertising agencies; companies and individuals in general.
There is a brief procedure with a conciliation hearing for the parties and the CONAR can impose sanctions, which include:
 - (i) correction or withdrawal of the advertisement, message or advertising campaign;
 - (ii) publicly admonishment of the sanctioned party, whether it is the sponsor of the advertising object of the complaint, the advertising agency that participated in its elaboration, if any, and the media through which it is broadcasted or disseminated;
 - (iii) suspension of CERNCO membership for up to one month; and
 - (iv) expulsion of the infringing party from CERNCO.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Paraguay?

All companies that are legally constituted in Paraguay and offer products and services are subject to the country's privacy regulations.

2.2 Does privacy law in Paraguay apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, privacy law is applicable to companies outside the country, provided that their activity affects individuals/corporations in the country. There are no specific obligations for such companies to have, eg, representatives in Paraguay; therefore, in case of actions taken against them, the matter is resolved under international private legislation (eg, the enforcement of a local judgement abroad).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Paraguay?

The Paraguayan Criminal Code defines 'intimacy' (private data) as the intimate personal sphere of a person's life, specially related to family, sexual life and state of health.

Under the Personal Credit Data Protection Law:

- (a) **Personal data** is information of any kind which refers to corporations or certain individuals that can be determined (determined as someone who can be identified). Protection of such personal data may be extended to corporations, where applicable; and
- (b) **Sensitive personal data** is data that refers to the intimate sphere of an individual/corporation or improper use of which may give rise to discrimination or entail a serious risk of the same.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

All information that refers to a person's intimacy, eg a person's state of health, sexual preferences, religious convictions and political preferences, may be considered 'sensitive data'. That is to say, all information other than what is registered within the Public Registry (such as a person's name and identification card number, address, date of birth, civil status, occupation or professional activity, place of work and telephone number) is considered a sensitive data. Sensitive data may even refer to a person's financial status.

Specifically, the Personal Credit Data Protection Law states that data related to the racial or ethnic origin of a person is considered sensitive, as well as information regarding a person's religious, philosophical and moral beliefs and convictions; political opinions; data related to health, life, sexual orientation and genetic or biometric data directed to identifying an individual.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

There are no specific rules that determine the treatment of anonymized, pseudonymized or de-identified data.

However, the Personal Credit Data Protection Law states that 'publicity or broadcasting of sensitive data related to persons that are expressly individualized or may be individualized is prohibited.' Therefore, *contrario sensu*, the publicity or broadcasting of data that is anonymous or de-intendified would be permissible. Pseudonymized data can be permitted, provided that the person to which the data belongs cannot be identified in any way or that it would be very hard to identify such person by means of the specific publicity or advertisement concerned.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Transparency and the protection of consumer rights.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, the Personal Credit Data Protection Law differentiates between 'bureaus of credit information' (namely, corporations that provide credit information and whose operation has to be authorized by the Paraguayan Central Bank) and 'users', who are users of credit information duly identified and who are provided with credit information by credit information companies.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

There are no specific rules to date regarding lawful basis for processing personal data in Paraguay.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

There are no information requirements that companies need to include in their privacy notices when processing personal data for advertising purposes.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the right to have their dignity respected and the right to not have their personal information publicized unless they have specifically consented to this.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

There are no specific norms regarding opt-out options from advertising activities nor the obtention of consent by individuals.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The use of cookies, pixels, etc, is not specifically addressed by the Paraguayan legislation.

Most marketing communications are not regulated from a privacy perspective.

However, there is a national Registry within SEDECO, in which consumers and users may request their names and data to be filed in order to prevent providers of any kinds of goods or services from contacting them on their mobile phone. Companies must consult this Registry to verify whether a person/user is registered on it, and refrain from sending any sort of messages to their mobile phone if they are registered on this 'do-not-call' Registry.

However, communications between companies and users undertaken where a contract has already been entered into between the parties are exempted from this.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Non to date.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Non in place to date.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing is not specifically regulated by the Paraguayan legislation.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies and their use is not specifically regulated in the Paraguayan legislation.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs are not specifically addressed by the Paraguayan legislation.

Promotions are regulated by Law No 7438/2025 (which modifies and broadens the scope of Law No 1016/1997), which sets the legal regime for the exploitation of games of chance, and are enforced by CONAJZAR, the National Commission of Games of Chance; however, there are no provisions which specifically address the protection of data and private data/personal data.

7.4 How is social media and influencer marketing regulated under privacy law?

There are no regulations in place related to the media and influencer marketing.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are no regulations related to targeted advertising.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no regulations related to digital identity resolution and clean room technologies.

7.7 How is location-based advertising regulated under privacy law?

There are no regulations related to location-based advertising.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific privacy laws governing data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

There are several restrictions, particularly for TV commercials and radio programs (timeframe, regarding the use of children in tobacco products and alcoholic beverages advertisement, etc).

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There is no provision to date that regulates the profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes in Paraguay.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes, there are requirements set out in the Personal Credit Data Protection Law regarding the international transfer of personal data to a recipient who is in a third country or to an international organization, when the guarantees, requirements or exceptions established in this Law are not met.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

None other than those mentioned above.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Paraguay? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is regulated as follows:

- (a) The Law on Electronic Trade determines that any provider of goods or services by electronic means, as well as hosting providers, amongst others, shall not make information available or accessible to third parties, except where there is a judicial order.
- (b) Privacy and data security are also protected at a Constitutional level.
- (c) Most importantly, the Personal Credit Data Protection Law provides that: ‘The corporation or individual responsible for personal credit data shall guarantee the adoption and implementation of technical, organizational and security measures, which are necessary to safeguard the access and integrity of personal data, in order to avoid its alteration, loss, consultation, commercialization or unauthorized access. And where such person or corporation gives an incomplete, late or defective notification to the authority in charge of data protection, information related to a personal data security breach, such corporation or individual shall be sanctioned according to the same law.’

There are no differences regarding the size of the entities or their sector: the same cannot broadcast or publicize personal data.

9.2 How are personal data breaches regulated in Paraguay? What are the requirements for notification and response?

Personal data cannot be publicized, disclosed, or broadcast; individuals have the legal remedies referred in question 1.4.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The potential penalties and sanctions for violations of privacy or data security regulations are usually fines and claims for damages, and, in some (very grave) cases, where a criminal complaint has been made, imprisonment.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes. Individuals may file complaints before the civil and the criminal courts.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

SEDECO is becoming more active and to date, we see more people filing complaints before said office for breach of the Consumer Protection Law. However, there are not yet many complaints and actions filed for breach of privacy. We do expect that with the passing of a specific law to regulate privacy and the establishment of a public entity for enforcement of such law, there will be more actions and more protection of individuals' privacy and personal data.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Paraguay?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

There is a Privacy Bill currently being studied by the Paraguayan Congress.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There have been no major changes since the last publication of this book. However, we do expect there to be a major change in the near future with the passing of a Privacy Law in Paraguay, currently being studied by the Congress.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

None to date. But companies will face challenges in the near future.

12.3 What do you envision the privacy landscape will look like in five years?

We think that there will be more regulations in place regarding privacy and the protection of the individual's private and personal data and a specific public entity in charge of the enforcement of the law.

PERU

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Peru.

Data privacy rights are regulated by the laws discussed at question 1.2.

1.2 What are the primary laws regulating privacy in Peru? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The Laws regulating privacy are:

- (a) Law 29,733 on Personal Data Protection ('PDP Law'); and
- (b) Supreme Decree 016-2024-JUS, which came into force on March 30, 2025, and replaces the previous Decree 003-2013-JUS approves the amendments to Regulations under the Law on Personal Data Protection ('PDP Regulations').

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Advertising practices are regulated by law. However, the PDP Law and the PDP Regulations establish that if companies implement a code of conduct and an impact assessment report on the processing of personal data carried out, they will mitigate any liability.

1.4 How is privacy law enforced in Peru? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Data privacy law is enforced by the General Directorate of Data Privacy Protection of the Ministry of Justice ('Data Privacy Authority').

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Peru?

The PDP Law and PDP Regulations apply to the processing of personal data, even if they are not in a personal data bank. They apply to all forms of personal data processing, whether carried out by natural persons, public entities or private sector institutions, regardless of the medium in which they are located. They apply whether or not particular or special rules or regimes also apply.

2.2 Does privacy law in Peru apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The provisions of the PDP Law and PDP Regulations are applicable to the processing of personal data when:

- (a) the processing is carried out in Peru;
- (b) the processing is carried out by a processor, regardless of its location, on behalf of a Peruvian personal data bank owner or data controller;
- (c) the owner of the personal data bank or controller is not established in Peruvian territory, but uses means located in Peru (unless such means are used only for transit purposes that do not involve the processing of personal data) in order to carry out activities:

- (i) related to the offer of goods or services aimed at owners of personal data located in Peru, or
- (ii) aimed at analyzing the behavior of the data owners located in Peru, or the development of profiles that seek to predetermine behaviors, preferences, habits or similar; or
- (d) the owner of the personal data bank or controller is not established in Peru, but Peruvian legislation is applicable, by contractual provision or international law.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Peru?

‘Personal data’ is the numerical, alphabetical, graphic, photographic, acoustic, personal habits, location, online identifiers or any other type of information concerning physical, economic, cultural or social aspects of natural persons that identifies them or makes them identifiable. Information is considered to be ‘identifiable’ when the identity of the individual can be verified directly or indirectly from the combination of data through means that can reasonably be used.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive personal data’ is information relating to genetic or biometric data of a natural person, neural data, moral or emotional data, facts or circumstances of their affective or family life, personal habits that correspond to the most intimate sphere, information relating to trade union membership, physical or mental health or other similar information that affect their privacy.

Regarding the processing of sensitive data, in addition to complying with the general requirements for valid consent, consent must be granted in writing, through handwritten, digital, electronic signature or any other modality that guarantees the will of the owner of the personal data.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

‘Dissociation’ is the procedure that prevents identification or does not make the owner of personal data identifiable. This procedure is reversible.

The person in charge of processing personal data must choose the appropriate technique when carrying out the dissociation procedure, always taking into account:

- (a) the type of data subject to processing,
- (b) the number of data subjects and
- (c) the risk factors (severity, probability, consequences for the controller and the owner) and those determined by the Data Privacy Authority for this purpose.

The Data Privacy Authority approves the complementary provisions for the implementation of the dissociation and anonymization procedure.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Databanks and data controllers must:
 - (i) register their databanks before the Data Privacy Authority;
 - (ii) inform the Data Privacy Authority of any cross-border data transfer flow;
 - (iii) have an adequate level of security to protect data from breaches;
 - (iv) in the event of a security incident that may compromise a large amount of data or number of persons, notify the Authority of the security incident within 48 hours of becoming aware of it; and
 - (v) post their terms and conditions and privacy policies on their websites so data subjects are aware of them;
- (b) Databank owners, data controllers and data processors have the following obligations:
 - (i) Carry out the processing of personal data, only with the prior informed, express and unequivocal consent of the personal data holder, except for authoritative law, with the exception of the assumptions set forth in article 14 of this Law;
 - (ii) Do not collect personal data by fraudulent, unfair or illegal means;
 - (iii) Collect personal data that is updated, necessary, pertinent and adequate, in relation to specific, explicit and lawful purposes for which they were obtained;
 - (iv) Do not use the personal data subject to process for purposes other than those that motivated its collection, unless there is an anonymization or dissociation procedure;
 - (v) Store personal data in a way that enables the exercise of the rights of its holder;
 - (vi) Delete and replace or, where appropriate, complete the personal data subject to process when becoming aware of its inaccurate or incomplete nature, without prejudice to the rights of the holder in this regard;
 - (vii) Delete the personal data subject to process when they are no longer necessary or relevant to the purpose for which they were collected or the term for their processing has expired, unless there is an anonymization or dissociation procedure;
 - (viii) Provide the Data Privacy Authority with the information regarding the processing of personal data that it requires and allow access to the personal data banks that it manages, for the exercise of its functions, within the framework of an administrative procedure in progress requested by the affected party;
 - (ix) appoint a personal data compliance officer; and
 - (x) appoint a representative in the Peruvian territory or for the Peruvian territory who will be the point of contact with the Data Privacy Authority.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

There are separate roles of data controller and data processor:

- (a) **Data controller:** The natural person, legal person under private law or public entity that decides on the purpose and means of the processing of personal data. This definition is not restricted to the owner of the database, but includes any person who decides on the processing of personal data, even if it is not in a personal data bank;

- (b) **Data processor:** The natural person, legal person under private law or public entity that processes data on behalf of, or by order of, the data controller or owner of the personal data bank.

However, the obligations and contractual requirements on database owners, controllers and processors are the same, as the processor assumes the obligations of the controller on its appointment.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, the personal data bank owner or controller must obtain consent for the processing of personal data. The request for consent must be in respect of a specific processing or series of processing, identifying the express purpose or purposes for which the data are collected.

Consent to the processing of personal data is valid only if the following characteristics are met, namely that the consent is:

- (a) free;
- (b) prior;
- (c) express and unequivocal; and
- (d) informed.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

When a person is contacted for marketing purposes for the first time, prior consent need not have been obtained. However, consent must be obtained in the first contact—otherwise no subsequent contact may be made.

When contact is first made with a person, their details may have been obtained from publicly-accessible sources; in such a case, the data controller must be in a position to inform the data subject, on request, of the source of the personal data.

It is presumed that the person processing personal data for advertising and commercial marketing is the person in whose interest such processing is carried out, unless proven otherwise. Where processing is carried out by someone else, the data controller must establish the necessary procedures to ensure that requests submitted to a data processor are forwarded to it in order to provide them with the appropriate attention.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

The owner of personal data has the right to refuse, revoke or oppose the processing of their personal data for advertising and commercial marketing purposes, and the data controller must provide a simple and free means to process such a request, which must be acted upon within ten days. The means by which they may refuse, revoke or oppose the processing of their personal data for advertising and commercial prospecting purposes should not be more complex than that used to grant consent.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Consent must always be obtained, despite the first contact mentioned in question 7.1.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The PDP Law does not specifically address the use of vendors and other third parties in advertising.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The processing of personal data may be carried out by a party other than the data processor, through an agreement or contract. If so, prior authorization is required from the owner of the personal data bank or data controller. Such authorization is understood to have been granted if it was provided for in the legal instrument by which the relationship between the controller and the processor was formalized. The treatment carried out by the subcontractor will be carried out in the name and on behalf of the data controller, but the burden of proving authorization lies with the data processor. The subcontractor then assumes the same obligations as those established for a data processor in the PDP Law, the PDP Regulations and other applicable provisions.

However, a third party assumes the obligations of the owner of a personal data bank when:

- (a) it destines or uses the personal data for a purpose other than that authorized by the owner of the database or data controller; or
- (b) it makes a transfer, in breach of the instructions of the owner of the personal data bank, even if it is for the conservation of said data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

When performing due diligence, it must be verified that companies have complied with the requirements regarding:

- (a) registration of the databank before the Data Privacy Authority;
- (b) inform the Data Privacy Authority of any cross-border data transfer flow;
- (c) obtaining consent and informing the data subject; and
- (d) appointment of a DPO.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Marketing communications are regulated by the Spam Law (Law No 28493) and, in order to comply with the law, the communication must include the word 'advertisement' in the subject, so that the data subject can identify it immediately and be aware of its content.

Data processing for advertising and commercial marketing of products and services is lawful when consent is obtained directly from the owner of the personal data. However, prior consent is not needed for first contact. Where a person is approached through direct marketing for the first time, if consent is not obtained, it is not lawful to make subsequent contact or process their personal data.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There is no specific law regulating tracking technologies; however, taking into consideration the PDP Law, data subjects must grant their consent in order to be tracked by online technologies, such as cookies.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific privacy rules governing loyalty programs and promotions. However, the PDP Law can apply to privacy matters related to loyalty programs and promotions. In practice, companies operating these kinds of programs and promotions must obtain consent from data subjects in order to use their personal information and to send them emails and notices and to use their consumer habits. Such consent is mandatory.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing are not regulated under the PDP Law. The general law will apply, depending on the case.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising and behavioral advertising are not specifically regulated in the PDP Law, nor the Advertisement Law. The general law will apply, depending on the case.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not regulated under Peruvian privacy law.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not regulated under Peruvian privacy law.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are not defined and regulated under Peruvian privacy law.

7.9 How is advertising to children and minors regulated under privacy law?

Peruvian Data Privacy Law does not address any related advertisement issue regarding children and minors. In this case, we will need to follow the rules of the Peruvian Advertisement Law.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The PDP Law does not address any related advertisement regarding profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes.

7.11 Are there other specific advertising practices that you wish to discuss?

No. The only specific advertising practices included in Peruvian privacy law is the one for processing for advertising and commercial marketing for which see question 7.1.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Data controllers and data processors may transfer personal data cross border only if the destination country maintains an adequate level of protection according to the PDP Law. Otherwise, in cases where the destination country does not provide adequate protection, the recipient must guarantee that the processing of personal data will conform to the requirements of the PDP Law. In the event that the country does not have the appropriate level of data protection, the issuer or exporter must provide adequate guarantees to the data subject to ensure the adequate processing of personal data outside the national territory.

To determine the appropriate level of data protection in a country, the Data Privacy Authority may issue a resolution upon request in order to determine whether the country has a protection comparable to the provisions of the PDP Law and PDP Regulations. The evaluation considers, inter alia:

- (a) the existence of a legal framework for the protection of personal data;
- (b) the existence of principles for the processing of personal data;
- (c) the existence of rules that recognize and guarantee the rights of data subjects and that they may have ways to exercise them; and
- (d) the existence of an authority in charge of the protection of personal data, or those that take its place, to supervise and sanction infringements of the regulations, when appropriate.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No. However, there are exemptions from the general rule; and guarantees are not required in the following situations:

- (a) when the data subject has given prior informed, express and unequivocal consent.
- (b) agreements within the framework of international treaties to which Peru is a party;
- (c) international judicial cooperation;
- (d) international cooperation among intelligence agencies for the fight against terrorism, illicit drug trafficking, money laundering, corruption and trafficking of persons and other forms of organized criminal activity;
- (e) when the personal data is necessary for the execution of a contractual relationship in which the data subject is a party, including where it is necessary for activities such as authentication of user, improvement and support of service, monitoring of quality of service, support for the maintenance and invoicing of the account and those activities that the management of the contractual relationship requires;
- (f) when related to bank or stock market transfers, in relation to the respective transactions and according to the applicable law;

- (g) when the cross-border flow of personal data is performed for the protection, prevention, diagnosis or medical or surgical treatment of the data subject, or when it is necessary for the performance of epidemiological or similar studies, as long as adequate dissociation procedures are applied; and

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Peru? Are there minimum standards? Does this differ by sector or size of the entity?

According to the PDP Law, a ‘personal data security incident’ is any breach of security that causes the destruction, loss, illicit alteration of personal data, or the unauthorized communication or exposure to said data.

In the event of a personal data security incident that results in the exposure of large volumes of personal data, in terms of quantity or type of data, or that may affect a large number of people, or when it involves sensitive data, or when there is obvious damage to other rights or freedoms of the owner of the personal data, the owner of the database or the person responsible for the processing must notify the Data Privacy Authority no later than 48 hours after becoming aware of or aware of it. If such notification is made later than this, the notification must be accompanied by an indication of the reasons and/or evidentiary support for such delay. This obligation remains even if the data controller considers that such an incident has been rectified or resolved internally.

9.2 How are personal data breaches regulated in Peru? What are the requirements for notification and response?

See answer to question 9.1.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) For minor infractions, a fine of up to two Tax Units;
- (b) For serious infractions, a fine of between two to six Tax Units; and
- (c) For very serious infractions, a fine of between six to ten Tax Units.

In the event of persistent non-compliance, a new periodic penalty payment may be imposed, successively doubling the amount of the last fine imposed up to the limit of 100 Tax Units.

(1 Tax Unit is approx USD 1,450.)

10.2 Do consumers have a private right of action? What remedies are available to them?

Data subjects have the rights of information, access, rectification, cancellation, opposition and objective processing of personal data. The rights may only be exercised:

- (a) by the owner of personal data, proving their identity and presenting a copy of their National Identity Document or equivalent document (The use of the digital signature in accordance with current regulations replaces the presentation of the National Identity Document and its copy);

- (b) through a legal representative accredited as such; or
- (c) by means of a representative expressly authorized to exercise the right, attaching a copy of their National Identity Document or equivalent document, and of the title that accredits the representation.

The exercise of one or more of the rights does not exclude the possibility of exercising one or more of the others, nor can one be understood as a prerequisite for the exercise of any of them.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The Peruvian Data Privacy Authority is very active and is always enforcing the law. The most common areas of enforcement concern:

- (a) registration of data banks;
- (b) communication of data transfers;
- (c) whether a company has privacy policies; and
- (d) whether consent to treat personal data has been obtained.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Peru?

N/A

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Companies must comply with the PDP Law. If they comply with their obligations, there will be no legal challenge of which they should be aware.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No. However, if a client needs more in-depth advice, please contact us.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

On November 30, 2024, Supreme Decree 016-2024-JUS, approving the DPD Regulations, was published. The Regulations are effective as of March 30, 2025.

In 2022, Peruvian privacy law did not apply to foreign companies. As from March 30, 2025, the PDP Law and PDP Regulations apply to data bank owners or data controllers that are not located in Peruvian territory, when they carry out activities:

- (a) related to the offer of goods or services aimed at personal data subjects located in Peruvian territory; and/or
- (b) aimed at analyzing the behavior of owners of personal data located in Peruvian territory, or the development of profiles that seek to predetermine behaviors, preferences, habits or similar.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

As from March 30, 2025 the law will be applicable to all companies, local or foreign, so they must be aware of the obligations they must comply in order to avoid infringements.

12.3 What do you envision the privacy landscape will look like in five years?

As the Law has recently changed, we do not envisage any amendment in the next five years. So the landscape will remain the same.

 PUERTO RICO

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Puerto Rico.

Puerto Rico has several laws and regulations related to privacy. These address issues such as:

- (a) the compulsory notifications of security breaches and privacy policies;
- (b) the disposal of personal information; and
- (c) prohibitions on the use of spyware.

Additionally, Puerto Rico has criminal laws prohibiting acts that result in the ‘violation of personal communications’ or in the ‘disclosure of personal information and data’.

1.2 What are the primary laws regulating privacy in Puerto Rico? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The key laws regulating privacy are:

- (a) Citizen Information on Data Banks Security Act (Act No 111-2005);
- (b) Privacy Policy Notification Act (Act No 39-2012);
- (c) Destruction of Personal Information Act of Puerto Rico (Act No 234-2014);
- (d) Puerto Rico Penal Code (Act No 146-2012);
- (e) Regulation of Spyware Act (Act No 165-2008);
- (f) Department of Consumer Affairs (‘DACO’) Regulation No 7367 regarding the Citizen Information on Data Banks Security Act;
- (g) DACO Regulation No 8568 on Privacy and Personal Information Protection;
- (h) Commonwealth of Puerto Rico Cybersecurity Act (Act No 40 of 2024); and
- (i) Cyber Privacy Protection Act for Children (Act No 185 of 2024).

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation enhances the protection of the company collecting the data by promoting compliance with industry standards and reducing legal risks. It also provides additional protection to persons in Puerto Rico by ensuring transparency, accountability, and responsible data handling practices.

1.4 How is privacy law enforced in Puerto Rico? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

- (a) The Citizen Information on Data Banks Security Act, the Privacy Policy Notification Act, the Destruction of Personal Information Act of Puerto Rico, DACO Regulation No 7367, and DACO Regulation No 8568 are all enforced via the Puerto Rico Department of Consumer Affairs. Individuals may file actions for civil damages based on these laws or on the Civil Code.
- (b) The Puerto Rico Penal Code and the Regulation of Spyware Act are enforced by the Government through the Department of Justice.
- (c) The Puerto Rico Innovation and Technology Service is responsible for ensuring the secure management of information resources and implementing information technology security standards and procedures at the government level under the Commonwealth of Puerto Rico Cybersecurity Act.

- (d) The Cyber Privacy Protection Act for Children is enforced by the Telecommunications Bureau of Puerto Rico, which has primary jurisdiction to address all complaints that may arise as a result of this Act and the authority to appeal to any court with jurisdiction to implement its resolutions and orders.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Puerto Rico?

The following are subject to privacy laws in Puerto Rico:

- (a) any company doing business that keeps a database containing customers' personal information is subject to privacy law in Puerto Rico;
- (b) any company that possesses, is in custody of, or controls archives that contain consumer personal information;
- (c) any Internet page operator in Puerto Rico; and
- (d) anyone subject to the jurisdiction of Puerto Rico and who violates the privacy provisions of the Puerto Rico Penal Code.

2.2 Does privacy law in Puerto Rico apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Privacy law in Puerto Rico does not apply to companies outside the country, except in the case of website operators.

Any operator of a website that is available in Puerto Rico must comply with the Privacy Policy Notification Act. This Act requires every Internet page operator to notify its users of its privacy policy in a clear, concise, conspicuous and unambiguous manner, so that users are able to know:

- (a) the type of personal information that the site gathers and/or stores when the page is accessed;
- (b) with whom it shares the personal information it gathers; and
- (c) the measures it has adopted to change or update its privacy policies and to notify such changes to its users.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Puerto Rico?

'Personal information' or 'personal data' is defined in several laws in Puerto Rico:

- (a) Under the Privacy Policy Notification Act, it includes any name or number that may be used by itself, or with any other information, to identify a specific person, including name, last name, social security number, date and place of birth, civil status, gender, address, email address, phone number, driver's license number, passport number, fingerprints, voice recordings, and retina images.
- (b) Under the Destruction of Personal Information Act of Puerto Rico it means any information that identifies, relates to, describes, or is capable of being associated with a particular person, including, but not limited to: paternal or maternal first name or first initial and last name; social security number; physical characteristics or descriptions; residential or mailing address; phone number; passport number; driver's license number or other official

identification; insurance policy number; education; employment; employment history; medical information or health policy; tax information; job evaluations; biometric data; bank or financial account number of any kind, with or without access codes that may have been assigned; credit or debit card number or any other financial information; usernames and passwords for computer systems; and data from 'black box' recording systems in motor vehicles. However, it does not include information that is disclosed to the general public under any state or federal law.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Under the Citizen Information on Data Banks Security Act, personal information considered sensitive includes: social security number; driver's license number; voter's identification number or other official identification; bank or financial account numbers of any kind, with or without associated passwords or access codes; usernames and passwords or access codes to public or private information systems; medical information protected by the HIPAA; tax information; and work-related evaluations, provided that this information is associated with a person's first name (or first initial) and surname.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Puerto Rico does not have specific local laws addressing the treatment of anonymized, pseudonymized, or de-identified data. Consequently, the handling of such data is generally guided by US federal regulations and industry best practices. For example, under federal laws like the HIPAA, de-identified data—where personal identifiers have been removed—is not subject to the same stringent privacy protections as identifiable data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Give notice to users regarding the privacy policy and any security breaches that may compromise personal data.
- (b) When disposing of personal information, the custodian must make sure that the personal information being discarded is not legible nor decipherable in any way.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Some privacy laws in Puerto Rico require consent:

- (a) The Cyber Privacy Protection Act for Children prohibits operators of internet pages or social media applications from publishing or disclosing personal information of those known to be minors residing in Puerto Rico without the consent of their parent or legal guardian, unless required by a court order or during a criminal investigation.

- (b) The Puerto Rico Penal Code prohibits any person who participates in a private personal communication from recording the communication without the express consent of all parties involved.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the Privacy Policy Notification Act, a website operator in Puerto Rico must:

- (a) state the type of personal information collected and/or retained about the site's users;
- (b) state any person or entity with whom the private operator shares the personal information collected and/or retained;
- (c) if the operator maintains a process for users to review or request changes to their personal information collected and/or retained, provide a description of that process;
- (d) describe a process by which the operator may notify its users of changes to its privacy policy. In such case, it must notify the date on which such change will take effect; and
- (e) state any other information that the Puerto Rico Department of Consumer Affairs deems relevant and compatible with the purposes of this Act.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Individuals have the right to be notified of the personal information being collected via a website, and of any security or data breach.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See question 5.1.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

As of 2025, Puerto Rico does not have a comprehensive data privacy law explicitly governing the use of vendors and third parties in advertising, such as advertising agencies, Demand-Side Platforms (DSPs), Supply-Side Platforms (SSPs), or data providers.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

As of 2025, Puerto Rico lacks a comprehensive data privacy law explicitly detailing contractual obligations for companies when disclosing or receiving personal data with vendors or third parties. However, certain sector-specific regulations and proposed legislation provide guidance on data handling practices:

- (a) The Commonwealth of Puerto Rico Cybersecurity Act establishes a framework to ensure cybersecurity within the Government of Puerto Rico and entities interacting with it. It applies to the Executive Branch, entities conducting business or holding contracts with the government, including, but not limited to, private entities performing public functions or services, and any administration involving public funds or resources. Under this Act, all Managed Service Providers (ie, entities that deliver services such as network, application, software, infrastructure, or security measures through ongoing, regular support and active administration on the premises of a government agency) must comply with the minimum cybersecurity standards outlined in the Act. Furthermore, any contract between a Managed Service Provider and a government agency must include measures to safeguard ‘sensitive assets’—defined as information, equipment, or media that, if lost, misused, or accessed or modified without authorization, could adversely affect government interests and/or citizens’ privacy. Additionally, government agencies must consult with the Puerto Rico Innovation and Technology Service prior to entering into any contract or amending, renewing, or extending a contract with a Managed Service Provider on the minimum cybersecurity requirements that the provider must meet to comply with the minimum cybersecurity standards outlined in the Act.
- (b) Under the Citizen Information on Data Banks Security Act, any entity that owns or guards a database that includes personal information of citizens residing in Puerto Rico must notify such citizens of any violation of system security when the databases whose security was violated contain, in whole or in part, their personal information files and the information is not protected with cryptographic keys beyond a password.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

As of 2025, Puerto Rico does not have a comprehensive data privacy law explicitly detailing due diligence measures or mandating impact assessments for advertising-related data processing.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

These matters are regulated by telemarketing laws in Puerto Rico.

The following will be considered prohibited or deceptive practices by any telemarketer or solicitor under the Telemarketing Fraud Prevention Act of Puerto Rico (Act No 210 of 2003):

- (a) failing to communicate, at the beginning of the call, text message, voice message, or AI message and before requesting any payment:
 - (i) the true purpose of the call, text message, voice message, or AI message,
 - (ii) the true name of the company or entity calling, sending the text message, voice message, or AI message, and
 - (iii) the goods or services offered;
- (b) failing to clearly and fully communicate the following information:
 - (i) the total cost to the consumer of the sale of the goods to be received,
 - (ii) any restrictions, limitations, or conditions on the purchase or use of the goods subject to sale,

- (iii) any terms or conditions in the seller’s cancellation, return, or exchange policy,
- (iv) any costs or conditions related to the awarding of prizes, including the odds of winning the prize, the nature and value of the prize, and
- (v) the exact amount of any offer;
- (c) failing to accurately disclose the quality and basic characteristics of the goods and services offered;
- (d) falsely advertising that the product or company in question is endorsed by any government entity or agency; or
- (e) requiring or subjecting a charge to a consumer’s bank account or credit card without the consumer’s authorization.

Also, US federal laws, such as the Telephone Consumer Protection Act of 1991, apply to these matters.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Under the DACO Regulation No 8568, website operators must disclose in their privacy policy how the website responds to ‘do not track’ signals.

7.3 How are loyalty programs and promotions regulated under privacy law?

In Puerto Rico, loyalty programs and promotions are primarily governed by advertising regulations aimed at preventing deceptive practices. The Puerto Rico Department of Consumer Affairs oversees advertising to ensure transparency and protect consumers from misleading marketing tactics. However, there is no comprehensive data privacy legislation specifically addressing the operation of loyalty programs and promotions.

7.4 How is social media and influencer marketing regulated under privacy law?

In Puerto Rico, social media and influencer marketing are primarily governed by advertising regulations aimed at preventing deceptive practices. The Puerto Rico Department of Consumer Affairs oversees advertising to ensure transparency and protect consumers from misleading marketing tactics. However, there is no comprehensive data privacy legislation specifically addressing the operation of social media marketing and influencer endorsements.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

N/A

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

N/A

7.7 How is location-based advertising regulated under privacy law?

N/A

7.8 How are data brokers defined and regulated under privacy law?

N/A

7.9 How is advertising to children and minors regulated under privacy law?

The Cyber Privacy Protection Act for Children prohibits operators of internet pages or social media applications from publishing or disclosing personal information of those known to be minors residing in Puerto Rico without the consent of their parent or legal guardian, unless required by a court order or during a criminal investigation.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Under the Telemarketing Fraud Prevention Act of Puerto Rico, certain practices related to telemarketing, including the use of artificial intelligence (AI) for messaging, are considered prohibited or deceptive if not properly disclosed. For example, the Act prohibits failing to communicate, at the beginning of the call, text message, voice message, or AI message and before requesting any payment the true purpose of the call, text message, voice message, or AI message.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There are no local laws addressing this matter, but personal data transfers across jurisdictions may be influenced by international regulations, particularly when data is transmitted from regions like the European Union to jurisdictions outside the European Union, including Puerto Rico. When transferring personal data from the European Union to Puerto Rico, entities may be required to utilize standard contractual clauses to comply with the EU General Data Protection Regulation (GDPR) requirements. This ensures that the data is protected in accordance with EU standards, even when processed outside the European Union.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

N/A

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Puerto Rico? Are there minimum standards? Does this differ by sector or size of the entity?

Data security and breach laws in Puerto Rico apply to personal information that is not protected with cryptographic keys beyond a password.

9.2 How are personal data breaches regulated in Puerto Rico? What are the requirements for notification and response?

Users must be informed of breaches as expeditiously as possible, taking into consideration the need for law enforcement agencies to secure possible crime scenes and evidence, as well as the application of measures needed to restore the relevant entity's cybersecurity system. Within a non-extendable term of 10 days after the breach has been detected, the entity concerned must inform the Department of Consumer Affairs of Puerto Rico, which must then make a public announcement of the breach within 24 hours of receiving the information. Individuals may file an action for damages if harmed by a breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

- (a) A fine of up to USD 5,000 for violations under the Citizen Information on Data Banks Security Act;
- (b) A fine of up to USD 50,000 for violations under the Privacy Policy Notification Act;
- (c) A civil penalty of up to USD 25,000 for each violation under the Cyber Privacy Protection Act for Children;
- (d) A fine of a fine of up to USD 5,000 or imprisonment for a term not exceeding 3 years for recording communications in violation of the Puerto Rico Penal Code;
- (e) A fine of up to USD 10,000 (if the violator is a legal entity) or imprisonment for a term not exceeding 3 years for a violation of personal communications in violation of the Puerto Rico Penal Code;
- (f) A Managed Service Provider (see question 6.2) who fails to comply with its obligations under the Commonwealth of Puerto Rico Cybersecurity Act will be subject to monetary penalties, which may be assessed up to the contract amount, along with any additional penalties specified in the contract or for other damages incurred, including those outlined in applicable local and federal law. In addition, neither the Managed Service Provider nor any other government agency substantially composed of the same people may be contracted by a government agency or government contractor, or as subcontractor for a period of five years.

10.2 Do consumers have a private right of action? What remedies are available to them?

Except for those laws enforced by the Department of Justice, the Telecommunications Bureau of Puerto Rico, or the Puerto Rico Innovation and Technology Service (see question 1.4), individuals may file actions for civil damages based on the privacy laws (see question 1.2) or on the Puerto Rico Civil Code. Injunctions and monetary relief may be obtained.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

There have been no widespread enforcement actions or legal cases specifically for privacy non-compliance related to advertising in Puerto Rico.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Puerto Rico?

While data privacy is a growing concern globally, consumer education about data privacy rights and protections may be less widespread in Puerto Rico. This could impact how effectively privacy laws are enforced, as individuals may not fully understand their rights under local or international privacy regulations.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

One topic to watch is the proposed Consumer Data and Personal Information Protection Act (Bill No 1548) which seeks to enhance the protection of personal data and privacy. Companies will need to prepare for stricter requirements around data collection, consent, and transparency, especially in terms of advertising and consumer interactions.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, the following privacy laws have been adopted:

- (a) The Commonwealth of Puerto Rico Cybersecurity Act, which was adopted to create a comprehensive cybersecurity framework between the Executive Branch of the Commonwealth of Puerto Rico, its agencies, departments, public corporations, and any natural or legal person doing business or having contracts with the Government; and
- (b) The Cyber Privacy Protection Act for Children, which was adopted to protect the well-being and integrity of children and to promote the peace of mind of Puerto Rico residents.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

As privacy laws and regulations continue to evolve in Puerto Rico, companies face multiple challenges that span regulatory compliance, data protection, cybersecurity, and consumer expectations. Staying ahead of these challenges requires ongoing adaptation to legal requirements, investment in technology and security, and maintaining clear communication with customers.

12.3 What do you envision the privacy landscape will look like in five years?

There is a possibility that the Consumer Data and Personal Information Protection Act (Bill No 1548) may be adopted (see question 11.2). Companies will need to prepare for stricter requirements around data collection, consent, and transparency, especially in terms of advertising and consumer interactions.

 RWANDA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Rwanda.

Rwanda's primary law governing privacy and data protection is Law No 058/2021 related to the protection of personal data and privacy, which came into effect on 15th October 2021. This law regulates how personal data is collected, stored, processed, and shared by organizations and companies, with an emphasis on ensuring transparency, consent, and security in handling personal data. It introduces significant safeguards for data subjects, grants them rights over their personal data, and provides a framework for handling data breaches.

1.2 What are the primary laws regulating privacy in Rwanda? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary legislation governing data protection in Rwanda is Law No 058/2021 ('Data Protection Law'), which ensures the rights of individuals to privacy, including consent, access, and rectification of personal data, together with its implementing regulations, focusing on specific sectors like healthcare, financial services, and education.

While there are no specific advertising laws in Rwanda's data protection regulations, the principles in the Data Protection Law apply to marketing and advertising practices. Data collected for marketing purposes is subject to the law's conditions on consent, data minimization, and transparency.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays a significant role in ensuring compliance with privacy standards, especially in advertising. While the law mandates compliance with privacy regulations, industry groups or advertising agencies may also implement internal codes of conduct to ensure that their practices align with ethical standards. This could include adopting best practices for obtaining consent for personalized advertising, using data responsibly, and ensuring transparency in the use of consumer data for marketing purposes.

1.4 How is privacy law enforced in Rwanda? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Rwanda Data Protection Office ('RDPO') is the main regulator responsible for enforcing the Data Protection Law. It oversees compliance, investigates breaches, and issues penalties for non-compliance. The RDPO has the authority to impose fines, penalties, and sanctions on non-compliant entities.

Industry groups may establish their own self-regulatory bodies or codes of conduct, particularly in advertising, to ensure compliance with the Data Protection Law.

Individuals may take legal action against organizations for violating their privacy rights, including seeking compensation for damages resulting from unlawful data processing.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Rwanda?

Under the Data Protection Law, a company is subject to Rwanda's data protection law if it processes the personal data of individuals within Rwanda, regardless of whether the company is based in Rwanda.

2.2 Does privacy law in Rwanda apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the law applies to foreign companies that process the personal data of Rwandan residents. Foreign entities must comply with Rwanda's privacy regulations if they engage in activities like online advertising targeting Rwandan citizens, or if they process data of individuals located in Rwanda. Foreign companies may be required to appoint a local representative within Rwanda to facilitate communication with the regulator and comply with local requirements.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Rwanda?

The Data Protection Law defines personal data as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Sensitive personal data includes information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details. Processing of sensitive data is subject to stricter conditions and requires explicit consent from the individual. The Data Protection Law lists the safeguards required when processing sensitive personal data which include the following:

- (a) compliance with requirements for personal data protection or personal data monitoring;
- (b) compliance with applicable sensitive personal data retention periods;
- (c) putting in place measures to strengthen capacities of staff involved in the processing of sensitive personal data;
- (d) putting in place measures to access sensitive personal data processed by the data controller or the data processor; and
- (e) implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed to the data subject, including, where appropriate, storing sensitive personal data separately from other types of data, and applying measures such as tokenization, pseudonymization or encryption.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Fully anonymized data is not considered personal data under the law as it does not identify individuals. However, pseudonymized or de-identified data still falls under the protection of privacy laws as it may still be linked back to an individual. Pseudonymization and de-identification are seen as security measures rather than a complete removal from the scope of the law.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Obtaining explicit consent before collecting personal data;
- (b) Implementing appropriate technical and organizational security measures;
- (c) Collecting only necessary data (data minimization principle);
- (d) Maintaining accurate and up-to-date personal data;
- (e) Limiting data retention periods;
- (f) Providing data subjects with access to their personal data;
- (g) Appointing a data protection officer for certain organizations;
- (h) Conducting data protection impact assessments ('DPIA's) for high-risk processing;
- (i) Reporting data breaches to the National Cybersecurity Authority;
- (j) Respecting data subjects' rights (access, rectification, erasure, etc);
- (k) Registering with the regulatory authority for certain processing activities;
- (l) Maintaining detailed records of all processing activities;
- (m) Ensuring all processing has a valid legal basis beyond just consent;
- (n) Establishing formal data processing agreements with third parties;
- (o) Following special provisions for collecting children's data;
- (p) Complying with direct marketing restrictions;
- (q) Adhering to limitations on automated decision-making; and
- (r) Supporting data portability between service providers.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

- (a) **Data controllers** are companies that determine the purposes and means of processing personal data;
- (b) **Data processors** are companies that process data on behalf of the controller.

These roles impact the company's obligations. For example, controllers are primarily responsible for ensuring compliance with the law, while processors must only act according to the controller's lawful instructions. The processing of data by a data processor must be subject to a written contract.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, privacy law requires a lawful basis for processing personal data. Under the law, processing of personal data must be based on one of the following lawful grounds:

- (a) **Consent:** The data subject has given clear, specific, and informed consent for the processing of their personal data for one or more specific purposes.

- (b) **Contractual necessity:** Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.
- (c) **Legal obligation:** Processing is necessary for compliance with a legal obligation to which the data controller is subject under Rwandan law.
- (d) **Vital interests:** Processing is necessary to protect the vital interests of the data subject or another natural person.
- (e) **Public interest:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- (f) **Legitimate interests:** Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

For sensitive personal data, the law imposes stricter requirements, generally requiring explicit consent or other specific conditions to be met Such as heightened security measures or specialized training for staff handling sensitive personal data.

The data controller bears the burden of demonstrating that they have a valid lawful basis for processing personal data, and this must be determined before the processing begins.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Companies must include the following in their privacy notices:

- (a) identity and contact details of the data controller and, where applicable, their representative or data protection officer;
- (b) purpose of processing—ie clearly stating that data will be used for advertising purposes, with specific details about the types of advertising (eg, targeted advertising, behavioral advertising);
- (c) categories of personal data being collected and processed;
- (d) lawful basis for the processing (whether consent, legitimate interest, or another legal ground);
- (e) recipients or categories of recipients with whom the data may be shared, including advertising partners, analytics providers, and other third parties;
- (f) data retention periods—ie how long the advertising data will be kept;
- (g) data subject rights, including the right to access, correct, delete data, object to processing, withdraw consent, and file complaints;
- (h) information about automated decision-making, including profiling, if used for advertising purposes, and the logic involved as well as potential consequences;
- (i) international data transfers: information about any transfers to countries outside Rwanda and the safeguards in place;
- (j) whether providing personal data is mandatory and the consequences of not providing it; and
- (k) the right to opt-out of advertising, especially for direct marketing.

For advertising specifically, the privacy notice should be particularly clear about:

- (l) how consumer behavior is tracked across websites or apps;
- (m) whether and how the company uses cookies or similar technologies;

- (n) whether the data is combined with information from other sources to create profiles; and
- (o) how targeted or personalized advertising works in practice.

Companies should ensure their privacy notices are comprehensive without being overwhelmingly long or complex.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumer rights include:

- (a) **Right to information:** Consumers have the right to be informed about how their personal data is being collected and used for advertising purposes in clear, understandable language;
- (b) **Right to access:** Consumers can request confirmation of whether their data is being processed and access to their personal data that companies hold for advertising purposes;
- (c) **Right to rectification:** Consumers can request correction of inaccurate personal data used in advertising profiles;
- (d) **Right to erasure:** Consumers can request the deletion of their personal data when it is no longer necessary for the purposes for which it was collected, or when they withdraw consent;
- (e) **Right to object:** Consumers have the specific right to object to the processing of their personal data for direct marketing purposes at any time, including profiling related to such direct marketing;
- (f) **Right to withdraw consent:** If the processing is based on consent, consumers have the right to withdraw that consent at any time, which should be as easy as giving consent in the first place;
- (g) **Right to data portability:** Consumers can request and receive their personal data in a structured, commonly used format that allows them to transfer this data to another service provider;
- (h) **Right not to be subject to automated decision-making:** Consumers have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal or similarly significant effects;
- (i) **Right to lodge a complaint:** Consumers can file complaints with Rwanda's data protection authority if they believe their rights have been violated; and
- (j) **Right to restriction of processing:** In certain circumstances, consumers can request the restriction of processing of their personal data.

For advertising specifically, these rights mean consumers should be able to:

- understand how their data is being used to target advertisements;
- access their advertising profiles;
- correct inaccurate information in these profiles;
- opt out of targeted advertising; and
- delete their profiles entirely.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

- (a) Companies must obtain explicit, informed consent when:
 - (i) using cookies or similar tracking technologies for non-essential purposes like advertising tracking;

- (ii) processing sensitive personal data for advertising (including health information, religious beliefs, political opinions, etc);
- (iii) engaging in behavioral advertising that involves profiling or tracking across multiple websites/services;
- (iv) conducting location-based advertising using precise geolocation data;
- (v) marketing to children under the applicable age threshold; and
- (vi) transferring personal data internationally for advertising purposes to countries without adequate data protection laws.

For valid consent, companies must implement:

- clear and specific information about the advertising activities before obtaining consent;
- affirmative action requirement (pre-checked boxes are invalid);
- granular consent options for different types of advertising activities;
- easy withdrawal mechanisms that are as simple as giving consent; and
- documentation of when and how consent was obtained.

(b) In contrast, opt-out mechanisms are generally sufficient for:

- (i) direct marketing through traditional channels (postal mail, telephone) based on existing customer relationships;
- (ii) email marketing to existing customers about similar products and services (though initial notice with opt-out must be provided); and
- (iii) non-intrusive contextual advertising that doesn't involve profiling.

For opt-out mechanisms, companies must provide:

- visible, accessible opt-out methods in each marketing communication;
- immediate effect of opt-out requests;
- record-keeping of all opt-out requests;
- regular updates to marketing databases to reflect opt-out choices; and
- simple opt-out procedures that don't require excessive steps or information.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

- (a) **Controller-processor relationship:** Data controllers (typically the advertisers or brands) remain primarily responsible for ensuring that all processing by vendors complies with Rwandan data protection law. Data processors (ad agencies, DSPs, SSPs, etc) must process data only according to the controller's documented instructions.
- (b) **Written agreements:** The law requires formal written contracts between controllers and any third-party processors. These agreements must specify the subject matter, duration, nature, and purpose of processing. They must also outline the types of personal data involved and categories of data subjects.
- (c) **Due diligence obligations:** Controllers must conduct due diligence before selecting vendors. They should only use processors that provide sufficient guarantees to implement appropriate technical and organizational measures.

- (d) **Vendor security requirements:** Third parties must implement appropriate security measures to protect personal data. This includes encryption, access controls, and other safeguards proportionate to the risks.
- (e) **Sub-processor restrictions:** Processors (like ad agencies) cannot engage sub-processors without the controller's authorization. When authorized, the same data protection obligations must flow down to sub-processors.
- (f) **Cross-border transfers:** When vendors are located outside Rwanda, additional safeguards are required. International transfers must comply with Rwanda's cross-border data transfer provisions.
- (g) **Joint controller provisions:** When multiple parties jointly determine purposes and means of processing (eg, co-branded campaigns), they are considered joint controllers. Joint controllers must have transparent arrangements defining their respective responsibilities.
- (h) **Data sharing transparency:** Privacy notices must disclose categories of third-party recipients. Data subjects should understand which vendors receive their data and for what purposes.
- (i) **Vendor management requirements:** Controllers must monitor vendor compliance. Regular audits or assessments may be required for high-risk processing activities.
- (j) **Liability framework:** Primary liability typically rests with the controller. However, processors can be directly liable for violations of their specific obligations. Data subjects can seek remedies against either party.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Specific contractual obligations apply to both the disclosing party (typically the data controller) and the receiving party (typically the data processor):

- (a) For companies disclosing data (controllers):
 - (i) **Written agreement:** Establish a formal, legally binding written contract before any data is shared;
 - (ii) **Purpose limitation:** Clearly define the specific purposes for which the data may be processed by the vendor;
 - (iii) **Processing instructions:** Provide documented instructions regarding all authorized processing activities;
 - (iv) **Scope definition:** Specify the subject matter, duration, nature, and scope of processing;
 - (v) **Data categories:** Identify the types of personal data being shared and categories of data subjects;
 - (vi) **Security requirements:** Mandate appropriate technical and organizational security measures;
 - (vii) **Confidentiality obligations:** Require confidentiality commitments from all personnel handling the data;
 - (viii) **Sub-processor management:** Include terms governing if/how the vendor may engage additional sub-processors;
 - (ix) **Data subject rights:** Require the vendor to assist with fulfilling data subject requests; and
 - (x) **Breach notification:** Establish clear timelines and procedures for security incident reporting.

- (b) For companies receiving data (processors):
 - (i) **Data processing limitations:** Process data only according to the controller's documented instructions;
 - (ii) **Purpose restrictions:** Ensure data is used only for the specified purposes;
 - (iii) **Security implementation:** Implement and maintain appropriate security measures;
 - (iv) **Staff management:** Ensure staff members are bound by confidentiality obligations;
 - (v) **Sub-processor controls:** Obtain authorization before engaging additional processors;
 - (vi) **Assistance obligations:** Help the controller comply with data subject rights requests;
 - (vii) **Deletion/return requirements:** Return or delete personal data at the end of the service provision;
 - (viii) **Audit co-operation:** Allow for and contribute to compliance audits by the controller;
 - (ix) **Compliance documentation:** Maintain records of all processing activities; and
 - (x) **Breach response:** Notify the controller of any data breaches without undue delay.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

- (a) Based on this framework, companies operating in Rwanda should implement the following due diligence measures:
 - (i) Register with the National Cybersecurity Authority ('NCSA') as a data controller/processor;
 - (ii) Appoint a data protection officer (if processing large volumes of data);
 - (iii) Maintain records of personal data processing activities;
 - (iv) Establish clear retention periods and data minimization practices;
 - (v) Implement appropriate technical and organizational security measures;
 - (vi) Obtain valid consent from data subjects when required; and
 - (vii) Have procedures for responding to data subject access requests.
- (b) Regarding impact assessments for advertising specifically, Rwanda's law requires data protection impact assessments ('DPIA's) when:
 - (i) Processing is likely to result in high risk to individuals' rights and freedoms;
 - (ii) Activities involve automated processing, including profiling, that produces legal effects; and
 - (iii) Processing occurs on a large scale involving special categories of data (such as ethnic origin, political opinions, or biometric data).

For advertising purposes, impact assessments would typically be required when:

 - (iv) Conducting targeted advertising using sensitive personal information;
 - (v) Implementing extensive user profiling across multiple platforms; and
 - (vi) Deploying new technologies for behavioral tracking or analysis.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Under Rwanda's Data Protection Law, direct marketing activities such as emails, texts, and push notifications are regulated with a focus on consent and transparency. Key provisions include:

- (a) **Consent requirements:** Companies generally need explicit, prior consent from individuals before sending direct marketing communications. This consent should be freely given, specific, informed, and unambiguous;
- (b) **Opt-out mechanism:** All direct marketing communications must include a clear and simple way for recipients to opt out of future messages. Companies must honor these opt-out requests promptly;
- (c) **Identification requirements:** Marketing messages must clearly identify the sender and provide contact information;
- (d) **Purpose limitation:** Personal data collected for direct marketing can only be used for that specific purpose unless additional consent is obtained;
- (e) **Data minimization:** Only necessary personal data should be processed for marketing purposes;
- (f) **Special categories:** Extra protections apply when using sensitive personal data for marketing purposes;
- (g) **Existing customer exception:** There is a limited exception for marketing similar products or services to existing customers, provided they are given an opportunity to object when their data is first collected and in each subsequent communication; and
- (h) **Regulatory oversight:** The NCSA oversees compliance with these regulations and can impose penalties for violations.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

- (a) **Transparency requirements:** Organizations must clearly inform users about any tracking technologies deployed on websites or applications, including their purpose and data collected
- (b) **Consent mechanism:** Prior informed consent is generally required before deploying tracking technologies that collect personal data, except where strictly necessary for providing a requested service.
- (c) **Data subject rights:** Individuals have rights to access, correct, and delete personal data collected through tracking technologies.
- (d) **Data minimization:** Organizations should only collect data necessary for the stated purpose and retain it for no longer than required.
- (e) **Security measures:** Adequate technical and organizational measures must be implemented to protect data collected through tracking technologies.
- (f) **Cross-border transfers:** Additional requirements apply when transferring data collected via tracking technologies outside Rwanda—eg, recipients must provide guarantees they will not transfer data to other parties without appropriate safeguards.
- (g) **Registration requirements:** Organizations using tracking technologies for significant data collection may need to register with the NCSA.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions typically involve significant personal data processing, triggering various compliance requirements including:

- (a) **Legal basis for processing:** Companies must establish a valid legal basis for collecting and processing customer data in loyalty programs, typically through:
 - (i) Explicit consent.
 - (ii) Contractual necessity.
 - (iii) Legitimate interests (balanced against individual rights).
- (b) **Transparency requirements:** Organizations must provide clear information about:
 - (i) What personal data is collected for the loyalty program.
 - (ii) How the data will be used (profiling, targeted offers, etc).
 - (iii) How long data will be retained.
 - (iv) Any third parties who may access the data.
- (c) **Purpose limitation:** Data collected for loyalty programs can only be used for the specified purposes disclosed to customers.
- (d) **Data minimization:** Only data necessary for operating the loyalty program should be collected.
- (e) **Storage limitation:** Clear retention periods should be established, with data deleted when no longer needed.
- (f) **Special considerations for automated processing:** If the loyalty program involves automated decision-making or profiling, additional safeguards apply.
- (g) **Child participation:** Special protections apply if loyalty programs target or include children.
- (h) **Data subject rights:** Members must be able to:
 - (i) access their loyalty program data,
 - (ii) correct inaccurate information,
 - (iii) delete their data/cancel membership, and
 - (iv) object to certain processing activities.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing activities are subject to the broader data protection framework. The regulation provisions include:

- (a) **Data collection and processing**
 - (i) social media marketing campaigns must have a valid legal basis (typically consent) for processing personal data.
 - (ii) data collected through social channels should be limited to what's necessary for the stated purpose.
 - (iii) special category data (like biometric or health information) used in targeting requires additional safeguards.
- (b) **Influencer marketing transparency**
 - (i) influencers and brands must be transparent about their relationship with users.
 - (ii) sponsored content should be clearly labeled as such. Influencers must explicitly identify sponsored content using terms like 'Ad,' 'Sponsored,' 'Promotion,' etc
 - (iii) collecting data through influencer channels requires proper disclosure. Disclosures should be visible without scrolling or clicking and not buried among hashtags or at the end of posts.

- (iv) users must be informed about how their data will be used when interacting with influencer content.
- (c) **Audience targeting and profiling**
 - (i) detailed profiling activities for social media campaigns may require impact assessments;
 - (ii) users should be informed about automated decision-making or profiling used in social media marketing;
 - (iii) special provisions apply when targeting vulnerable groups or minors.
- (d) **User-generated content**
 - (i) marketing campaigns soliciting user content must obtain appropriate permissions from the users for the use of the content, including clear mechanism for users to withdraw permission;
 - (ii) clear terms should govern how user-submitted content may be used in marketing;
 - (iii) users should retain rights to request removal of their content.
- (e) **Cross-border considerations**
 - (i) when marketing campaigns collect data for processing outside Rwanda, additional transfer requirements apply.
 - (ii) international influencer campaigns must comply with Rwandan law when targeting Rwandan residents.
- (f) **Platform-specific compliance**
 - (i) organizations remain responsible for compliance even when using third-party social platforms;
 - (ii) privacy settings and data protection options should be respected even when technically possible to bypass them.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Rwanda's privacy framework, addresses targeted and contextual advertising through several provisions:

- (a) **Targeted advertising (behavioral or personalized):** Targeted advertising using personal data in Rwanda is subject to stringent requirements:
 - (i) The law mandates explicit prior consent before processing personal data for targeted advertising purposes, especially when building individual profiles;
 - (ii) Data controllers must provide comprehensive information about the processing purposes, including specific details on how behavioral data will be used to generate personalized advertisements;
 - (iii) Organizations conducting targeted advertising must implement appropriate technical and organizational measures to protect personal data collected and processed for advertising purposes;
 - (iv) The law recognizes individuals' right to object to processing for direct marketing purposes, which extends to targeted advertising activities; and
 - (v) When targeted advertising involves automated decision-making that produces legal or similarly significant effects, additional protections apply, potentially requiring human intervention.

- (b) **Contextual advertising:** Contextual advertising receives less restrictive treatment under Rwanda’s privacy framework. Since contextual advertising does not necessarily rely on processing personal data (focusing instead on content themes or keywords), it may fall outside certain provisions of the data protection law. In particular:
- (i) The legal requirements are significantly reduced when advertising is based solely on the current context of user activity rather than historical behavioral data or personal profiles;
 - (ii) Organizations may potentially rely on legitimate interests rather than explicit consent when displaying advertisements based strictly on current content consumption; and
 - (iii) Record-keeping and documentation requirements are likely less onerous for purely contextual advertising systems.

Rwanda’s regulatory framework for advertising is still developing, with the NCSA continuing to issue implementing regulations. In practice, organizations should:

- clearly distinguish between contextual and behavioral advertising approaches in their data processing records;
- document the legal basis for each type of advertising conducted;
- implement separate consent mechanisms specifically for behavioral advertising activities; and
- ensure privacy notices explicitly address both advertising methodologies when applicable.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

The Law does not explicitly mention these technologies, but several principles and provisions in the law apply to how they must be implemented:

- (a) **Digital identity resolution:** Digital identity resolution technologies, which link consumer identities across devices and platforms, face these regulatory considerations:
- (i) **Lawful basis requirements:** The fundamental requirement is establishing a valid legal basis for processing. For identity resolution, which often involves tracking and profiling, companies typically need to rely on either: Explicit consent from data subjects, especially when linking previously separate datasets or legitimate interest (though this requires a careful balancing test against individual privacy rights);
 - (ii) **Purpose limitation challenges:** Identity resolution must adhere to the purpose limitation principle. This means the original collected data must have been obtained for purposes compatible with identity resolution, new uses of combined data require consideration of whether they align with the original collection purposes and secondary uses may require fresh consent or notification;
 - (iii) **Transparency obligations:** Companies must provide transparent information about identity resolution practices, including clear explanation of how identities are linked across platforms; disclosure of the types of identifiers used (cookies, device IDs, hashed emails, etc); and information about how the resolved identities will be used; and
 - (iv) **Profiling restrictions:** Identity resolution often enables more sophisticated profiling, which triggers additional requirements for example data subjects must be informed about the existence of profiling; companies must implement mechanisms for individuals to object to profiling; automated decision-making based on profiles may trigger specific protections

- (b) **Data Clean Rooms:** Data clean rooms, which allow multiple parties to analyze combined datasets without directly sharing raw data, intersect with Rwandan privacy law in several ways:
 - (i) **Controller-processor relationships:** The clean room provider typically acts as a processor, requiring clear data processing agreements with participating companies; documented instructions on permitted processing activities and security guarantees appropriate to the sensitivity of the data involved;
 - (ii) **Data minimization implementation:** Clean rooms should be designed to embody data minimization by limiting the data elements brought into the clean room to those necessary for analysis; aggregating results to prevent individual-level data from leaving the clean room; and implementing query limitations to prevent re-identification attempts;
 - (iii) **Privacy by design integration:** Rwandan law embraces privacy by design principles, which clean rooms must incorporate through default privacy-preserving settings; technical safeguards against data leakage; and risk assessments before implementing new analytical capabilities; and
 - (iv) **Cross-border considerations:** When clean rooms involve international data flows, data transfer restrictions may apply if the clean room is hosted outside Rwanda. Additional safeguards may be necessary to legitimize these transfers and joint controller arrangements may need to account for different jurisdictional requirements.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising involves processing users' geolocation data, which is subject to strict privacy requirements under Rwanda's Data Protection Law. Key requirements applicable to location-based advertising include:

- (a) **Consent requirement:** Companies must obtain explicit and informed consent from individuals before collecting, processing, or using their location data for advertising purposes. This means users must be clearly informed about how their data will be used and must actively agree to it;
- (b) **Transparency:** The purpose of collecting location data must be clearly stated, and individuals must be informed about how their data will be used for advertising;
- (c) **Purpose limitation:** Location data can only be collected and processed for specific, legitimate purposes disclosed to the individual. It cannot be repurposed for unrelated activities without additional consent;
- (d) **Data minimization:** Companies are required to collect only the minimum amount of location data necessary for the stated purpose. Excessive or irrelevant data collection is prohibited;
- (e) **Security and safeguards:** Organizations must implement appropriate technical and organizational measures to protect location data from unauthorized access, breaches, or misuse;
- (f) **User rights:** Individuals have the right to access, correct, or delete their location data. They can also withdraw consent at any time, after which the data must no longer be used for advertising. Users must be provided with clear and easy-to-use mechanisms to exercise these rights;

- (g) **Accountability and compliance:** Companies engaging in location-based advertising must ensure compliance with the Data Protection Law and may be subject to audits or investigations by the NCSA, which oversees data protection in Rwanda. Non-compliance can result in penalties, including fines and other sanctions; and
- (h) **Cross-border data transfers:** If location data is transferred outside Rwanda, the recipient country must provide an adequate level of data protection, or additional safeguards must be implemented to ensure privacy.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are entities who collect, process, and trade personal data obtained from various sources, often for commercial purposes such as marketing, analytics, or advertising. Although data brokers are not explicitly defined or separately regulated under the current privacy law framework, data broker activities would fall under the scope of Data Protection Law. Under this law, entities that collect and sell personal data (which would include data brokers) would be considered data controllers and data processors and must:

- (a) register with the Rwanda data protection office ('RDPO') if they are involved in the processing of personal data;
- (b) ensure that they comply with data protection principles, such as transparency, data security, data minimization and consent, especially if they process sensitive data; and
- (c) conduct regular audits and implement data protection measures to avoid misuse of personal data.

7.9 How is advertising to children and minors regulated under privacy law?

The Data Protection Law requires special consideration for vulnerable groups, which would include children. General requirements that apply for advertising to children and minors include:

- (a) **Parental/guardian consent:** Companies must obtain the consent of a holder of parental responsibility over the child or minor below 16 years;
- (b) **Age verification:** Companies may need to verify the age of users to ensure compliance with age-specific advertising restrictions; and
- (c) **Content restrictions:** Advertising aimed at children must adhere to specific content restrictions to prevent exploitation or harm.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Rwanda's Data Protection Law establishes general data protection principles but doesn't specifically address AI or automated decision-making in great detail.

Key aspects of Rwanda's approach include:

- (a) **Transparency:** Companies must inform individuals if their data will be used for profiling, especially for automated decision-making in advertising.
- (b) **Consent:** Explicit consent is required when profiling is used for targeted advertising, particularly if the decision-making process significantly affects the individual (eg, credit scoring or personalized promotions).
- (c) **Right to object:** Individuals have the right to object to profiling, especially if it leads to decisions that are solely based on automated processing.

7.11 Are there other specific advertising practices that you wish to discuss?

Additional advertising practices that may be subject to privacy law include affiliate marketing, advertising via mobile apps, and video marketing. Each of these practices involves collecting personal data and, therefore, requires adherence to the established privacy principles—transparency, consent, purpose limitation and data security amongst others.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Under Rwanda's Privacy Law, cross-border data transfers are permitted but subject to specific conditions:

- (a) **Adequacy assessment:** Data transfers to other countries are allowed if the recipient country ensures an 'adequate level of protection' for personal data. However, Rwanda hasn't published an official list of countries that it deems to have adequate levels of protection.
- (b) **Transfer mechanisms:** The law allows for transfers when:
 - (i) the data subject has explicitly consented to the transfer;
 - (ii) the transfer is necessary for contract performance;
 - (iii) the transfer is necessary for public interest purposes; or
 - (iv) the transfer is necessary to protect the vital interests of the data subject
- (c) **Safeguards:** The law envisions the use of appropriate safeguards for transfers, though it does not explicitly detail mechanisms like Standard Contractual Clauses. Organizations typically use contractual mechanisms to ensure compliance, but Rwanda has not issued standard templates.
- (d) **Prohibited transfers:** The law does not explicitly ban transfers to specific countries, but the regulatory authority (RURA) has the power to restrict transfers to countries that do not provide adequate protection.
- (e) **Notification requirements:** Data controllers must notify the data protection authority before transferring data outside Rwanda.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

There are several additional considerations beyond basic compliance with Rwanda's data protection law:

- (a) **Professional privilege concerns:** eg, legal professional privilege/attorney-client privilege may restrict certain data transfers involving legal communications; medical data transfers might be subject to additional professional confidentiality requirements and banking secrecy laws could affect financial data transfers;
- (b) **Sector-specific requirements:** Financial sector data may have additional transfer restrictions under financial regulations; healthcare information might require specific safeguards beyond general data protection rules and telecommunications data could be subject to separate regulatory frameworks;
- (c) **National security considerations:** Rwanda's government may restrict transfers of certain data categories deemed sensitive for national security and critical infrastructure information might face additional scrutiny.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Rwanda? Are there minimum standards? Does this differ by sector or size of the entity?

Rwanda's Law establishes general security requirements rather than highly specific technical standards. Key aspects of Rwanda's data security regulation include:

- (a) **General security obligations:** Data controllers and processors must implement 'appropriate technical and organizational measures' to protect personal data. Security measures should be proportionate to the risks presented by processing. Organizations must consider the nature, scope, and purpose of processing when determining security measures;
- (b) **Minimum standards:** The law doesn't prescribe detailed technical standards or specific security technologies. Instead, it takes a risk-based approach that requires adequate protection against unauthorized access, disclosure, alteration, or destruction. Organizations are expected to implement measures like access controls, encryption, and data backup systems;
- (c) **Sector-specific variations:** for example, banks and financial institutions, telecom providers and those processing medical data are subject to additional requirement;
- (d) **Entity size considerations:** The law doesn't explicitly exempt smaller entities from security requirements. However, the 'appropriate measures' standard implicitly recognizes that implementation will vary based on organization size and resources. Small businesses are still expected to maintain basic security controls; and
- (e) **Breach notification:** Organizations must notify the data protection authority of serious breaches that may pose a risk to the rights and freedoms of natural persons. These include breaches that may lead to identity theft or fraud, breaches that may result in financial loss or damage to reputation and breaches affecting large volumes of personal data, regardless of sensitivity, amongst others.

9.2 How are personal data breaches regulated in Rwanda? What are the requirements for notification and response?

For data breach notifications and response, Rwanda's requirements include:

- (a) **Notification timeframe:** Data controllers must notify the NCSA of a personal data breach within 72 hours of becoming aware of it.
- (b) **Content of notification:** The notification must include:
 - (i) nature of the breach;
 - (ii) categories and approximate number of affected data subjects;
 - (iii) categories and approximate amount of affected personal data records;
 - (iv) contact details of the data protection officer or other contact point;
 - (v) description of likely consequences of the breach; and
 - (vi) measures taken or proposed to address the breach and mitigate potential adverse effects.
- (c) **Subject notification:** When a breach is likely to result in high risk to the rights and freedoms of individuals, the data controller must also notify affected data subjects without undue delay.
- (d) **Documentation:** Data controllers must document all personal data breaches, including facts about the breach, its effects, and remedial actions taken.
- (e) **Penalties:** Non-compliance with breach notification requirements can result in administrative fines imposed by the NCSA.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The law establishes several penalties for non-compliance with privacy regulations:

- (a) **Administrative penalties:** The NCSA can:
 - (i) impose administrative fines of up to 5% of the annual global turnover or specific monetary amounts (ranging from approximately 500,000 to 5,000,000 Rwandan Francs (approximately USD 360 to USD 3,600), depending on the violation) for organizations that fail to comply with various provisions of the law.
 - (ii) issue warnings and reprimands;
 - (iii) order temporary or permanent bans on processing;
 - (iv) order rectification or erasure of data; and
 - (v) suspend data flows to recipients outside Rwanda.
- (b) **Criminal penalties:** More serious violations can lead to criminal sanctions, including:
 - (i) Prison terms ranging from 6 months to 3 years
 - (ii) Fines ranging from 1,000,000 to 5,000,000 Rwandan Francs (approximately US\$ 710 to US\$ 3,600)
- (c) **Individual compensation:** Individuals who suffer material or non-material damage due to violations have the right to claim compensation from the data controller or processor.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers have the right to seek compensation for harm caused by unlawful processing of their data. Remedies include:

- (a) financial compensation for actual damages suffered;
- (b) orders to correct, complete, update, or delete personal data;
- (c) orders to cease unlawful processing activities; and
- (d) orders to comply with data subject rights (access, correction, deletion).

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement actions by the RDPO and other authorities are increasing, with fines and sanctions imposed on entities that violate privacy regulations, particularly in advertising contexts.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Rwanda?

Some cultural considerations influence privacy law and enforcement in Rwanda:

- (a) **Collectivist social structure:** Rwanda has traditionally emphasized community values over individual rights. This cultural orientation has shaped how privacy is conceptualized - often as a balanced consideration between individual rights and community interests rather than absolute individual privacy.
- (b) **Post-genocide context:** Following the 1994 genocide, Rwanda developed heightened sensitivity around data collection related to ethnic identities. This historical context has influenced strong protections against certain types of data collection and processing.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

AI in advertising, cross-border data transfers and biometric data processing are some of key legal challenges companies should monitor. Rwanda’s ambitions as a digital economy may create tension between promoting innovation and ensuring robust privacy protections.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

None

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Rwanda has seen an increased focus on data protection awareness and enforcement, with the Data Protection Office becoming more active in regulating digital advertising.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Adapting to consent management practices and ensuring data security in advertising activities, particularly when using third-party vendors.

12.3 What do you envision the privacy landscape will look like in five years?

We envision Rwanda’s privacy landscape in five years developing along these lines:

- (a) **Strengthened regulatory framework:** The NCSA will likely mature into a more assertive regulator with clearer enforcement guidelines and precedents. There will probably be more detailed implementing regulations that clarify ambiguities in the current law.
- (b) **Increased enforcement activity:** We expect more formal enforcement actions with financial penalties, particularly targeting multinational companies and data-intensive sectors like telecommunications and financial services.
- (c) **Digital identity integration:** Rwanda’s digital ID system (Irembo) will probably become more central to privacy considerations, with clearer rules about how digital identity data can be used in both public and private sectors.

SERBIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Serbia.

Privacy is regulated by a number of binding laws, bylaws, and other forms of regulations adopted on the national level. However, Serbia made important steps in increasing the level of data protection and reaching EU standards by adopting a *lex generalis* in 2018, which is based on the EU's GDPR and Police Directive. It is important to emphasize that the work on the privacy regulatory framework is yet to be completed. The Serbian Law on Personal Data Protection (the 'LPDP') prescribed that:

- (a) the provisions of other laws relating to the processing of personal data must be harmonized with the provisions of the Law by the end of 2020, and
- (b) the bylaws introduced with the Law must be adopted by August 21, 2019.

However, only the latter has been carried out, and therefore the Serbian legal framework still includes a number of laws not fully harmonized with the provisions of the LPDP.

1.2 What are the primary laws regulating privacy in Serbia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The principal law regulating privacy in the Republic of Serbia is the LPDP, based on the GDPR and the Police Directive.

The LPDP regulates:

- the right of natural persons to the protection of personal data in relation to its processing and the free flow of such data;
- the principles of processing;
- the rights of the data subject;
- the obligations of controllers and processors of personal data;
- the codes of conduct that may be prepared by associations and other bodies representing categories of controllers or processors;
- the transfer of personal data to other States and international organizations;
- supervision of the implementation of the Law;
- remedies, liability and penalties in the event of a violation of the rights of natural persons in relation to the processing of personal data; as well as
- special cases of processing.

Additionally, it regulates the right to the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating and detecting criminal offenses, prosecuting offenders or committing criminal sanctions, including prevention and protection against threats to public and national security, as well as the free flow of such data.

However, there are a number of other sector-specific laws which are important for regulating privacy, including:

- (a) Advertising Law—which regulates the necessity of obtaining prior consent from the person whose personal goods, including personal data, are contained in an advertisement;
- (b) Information Security Law—which regulates the use of personal data in the ICT systems, and its protection; and
- (c) Criminal Code—which prescribes criminal offenses related to the violation of personal data.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The Advertising Law stipulates that advertising must be conducted in accordance with the law, other regulations, good business practices, professional ethics, and other forms of self-regulation. It specifically provides for the independent regulation of business rules, ie, self-regulation, as a set of rules defining procedures in commercial communication, which includes advertising related to one or more business practices or industries, as well as professional standards. These business rules are established by all advertising participants, who are responsible for their formulation, adoption, implementation, monitoring, and revision.

Additionally, a self-regulatory body in the field of advertising ('NAESO') has been established to provide professional advice and interpretations regarding the application of the Code of Marketing Communications, review complaints about advertisements and campaigns, and organize educational programs.

1.4 How is privacy law enforced in Serbia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

- (a) **Commissioner for Personal Data Protection ('Commissioner').** This regulatory body is the most important player for privacy law enforcement. The Commissioner is a supervisory authority that acts, in accordance with the LPDP, in the territory of the Republic of Serbia. The Commissioner supervises and enforces privacy law in accordance with its authority, and promotes public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data.
- (b) **Competent courts.** The courts also play a crucial role in privacy law enforcement. In the case of a data breach, any natural or legal person, including a data subject, processor or controller, has the right to appeal against a legally binding decision of the Commissioner concerning them, or, where the Commissioner does not render a decision within 60 days from the day of the receipt of a complaint, to initiate an administrative court proceedings by filing a lawsuit with the Administrative Court. Additionally, a data subject has a right to initiate court proceedings before a competent court if they consider that the controller or processor has infringed their rights when processing personal data.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Serbia?

Privacy law in Serbia applies to all companies that have their headquarters in the territory of the Republic of Serbia and process personal data as controllers or processors within the framework of activities carried out in Serbia, regardless of whether the processing is itself carried out in Serbia. However, privacy law also applies to companies that do not have their headquarters in Serbia, but which process personal data as controllers or processors, if the processing is related to:

- (a) the offer of goods or services to a data subject in Serbia, regardless of whether that person is required to pay for these goods or services; or
- (b) monitoring the activities of data subjects, if the activities are carried out in Serbia.

2.2 Does privacy law in Serbia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Privacy law in Serbia applies to companies outside the country in the circumstances set out in question 2.1. In these cases, the company is obliged to designate, in writing, a representative in the Republic of Serbia, unless the processing:

- (a) is done only occasionally,
- (b) does not include to a great extent the processing of sensitive data, or
- (c) is unlikely to cause risk to the rights and freedoms of individuals.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Serbia?

‘Personal data’ is defined as any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

According to the national law, the following categories of personal data are considered as sensitive:

- (a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- (b) genetic data;
- (c) biometric data, in cases when it is processed for the purpose of uniquely identifying a natural person;
- (d) data concerning health; and
- (e) data concerning a natural person’s sex life or sexual orientation.

In general, the processing of sensitive data is prohibited, unless one of the limited number of exceptions provided in the LPDP applies.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Pseudonymized data is subject to the LPDP and is treated as personal data. The LPDP defines pseudonymization as processing in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to technical, organizational and staff-related measures to ensure that the personal data cannot be attributed to an identified or identifiable person.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

In general, privacy law is based on fundamental principles aimed at achieving and maintaining the following during data processing:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality.

The following obligations can be highlighted as key obligations for companies required by privacy law:

- (a) **Posting a privacy policy.**
- (b) **Keeping records of processing operations:** Both the controller and processor are obliged to keep records of processing operations. Namely, each controller and, where applicable, the controller's representative, is obliged to maintain a record of processing activities under its responsibility.
Records also must be kept by each processor/processor's representative with regard to all categories of processing activities carried out on behalf of a controller.
Records must be in writing, including in electronic form. Exception to the obligation to keep records of processing operations in certain cases where the controller and processor are companies or organizations with less than 250 employees.
- (c) **Conducting risk impact assessments and seeking prior consultation:** The controller is obliged, where processing is likely to result in a high risk to the rights and freedoms of natural persons, to carry out, prior to the processing, an impact assessment of the envisaged processing operations on the protection of personal data.
If the risk impact assessment indicates that the processing would result in a high risk, the controller is obliged, in the absence of measures taken by the controller to mitigate the risk, to consult the Commissioner as supervisory authority prior to processing.
- (d) **Appointing a privacy officer:** The controller/processor is obliged to designate a data protection officer in any case where the processing is carried out by a public authority or body, except in limited number of cases provided in the LPDP.
Once a privacy officer is appointed, the controller or the processor is obliged to publish the contact details of the data protection officer and communicate them to the Commissioner as supervisory authority.
- (e) **Informing data subject and Commissioner about a data breach:** The controller is obliged to notify a personal data breach to the Commissioner, as supervisory authority, without undue delay, or, where feasible, not later than 72 hours after having become aware of it. In addition, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is obliged to communicate such breach to the data subject without undue delay, except in cases defined by law.
A processor is obliged to notify the controller without undue delay after becoming aware of a personal data breach.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

In general, there is a difference between companies which act as controllers and the ones that act as processors:

- (a) **Companies acting as controllers:** These companies determine the purpose, and the method of the data processing and are responsible for and able to demonstrate compliance with all

key privacy principles, such as lawfulness, fairness and transparency, purpose limitation, data minimization, etc. These companies decide, within the legal framework, which data will be collected, for what period it will be kept, whether it will be shared with third parties, etc.

- (b) **Companies acting as processors:** These companies simply process the personal data and decide how it is stored. Consequently, they cannot change the purpose of the processing determined by the controller. It should be noted that processors process data only according to the controller's requirements set down in a contract or other legal act concluded between the controller and processor in writing, that is binding on the processor with regard to the controller. This contract must set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

The processor is obliged to inform the controller if any of the instructions contained in the contract constitutes an infringement of the law regulating data protection. Additionally, processors are obliged to inform controllers without undue delay when a data breach takes place.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

One of the fundamental principles on which privacy law is based is the principle of lawfulness, which requires that personal data must be processed lawfully, ie, in accordance with the provisions of the LPDP and other regulations governing the processing of personal data.

The LPDP provides the following as possible legal bases for data processing:

- (a) **Consent:** The data subject gives consent for one or more specifically defined purposes of processing;
- (b) **Contract:** Processing is necessary for the performance of a contract concluded with the data subject or for taking steps at the request of the data subject prior to entering into a contract;
- (c) **Legal obligation of the controller:** Processing is necessary for compliance with the controller's prescribed legal obligations;
- (d) **Vitally important interests:** Processing is necessary to protect vitally important interests of the data subject or another natural person;
- (e) **Public interest:** Processing is necessary for performing tasks in the public interest or exercising legally prescribed powers of the controller; and
- (f) **Legitimate interest of the controller or a third party:** This refers to a real, specific, and legally permissible interest of the controller or a third party, for which the processing of certain personal data is necessary, provided that such interest does not override the interests or fundamental rights and freedoms of the data subject.

For data processing to be lawful under the LPDP, the controller must determine, in each specific case, the legal basis for processing that corresponds to the specific circumstances under which the processing takes place.

However, the controller must also ensure that the lawfulness of a particular processing activity is not limited to merely selecting the appropriate legal basis. It also includes compliance with all other processing principles outlined in question 4.1, as well as fulfilling all legal obligations, such as maintaining records of processing activities, appointing a data protection officer, and other requirements prescribed by law.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Where personal data relating to a data subject is collected from the data subject, the controller is obliged, at the time when personal data is collected, to provide the data subject with the following information:

- (a) on the identity and on the contact details of the controller as well as on the controller's representative, where he/she has been designated;
- (b) the contact details of the person tasked with personal data protection, where he/she has been designated;
- (c) on the purpose of the intended processing and on the legal basis for the processing;
- (d) on the existence of a legitimate interest pursued by the controller or a third party;
- (e) on the recipient and/or on the group of recipients of the personal data, if any;
- (f) on the fact that the controller intends to transfer personal data to another country or to an international organization.

Also, in order to ensure fair and transparent processing, it is necessary to provide data such as:

- (g) the retention period of personal data or, if that is not possible, the criteria for determining it;
- (h) information about the rights of individuals to request access, correction, or deletion of their personal data, the right to object, as well as the right to data portability;
- (i) indication of the existence of the right to withdraw consent at any time, as well as that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal;
- (j) the right to lodge a complaint with the Commissioner;
- (k) information about whether providing personal data is a legal or contractual obligation, or if providing data is a necessary condition for entering into a contract, as well as whether the individual to whom the data relates is obligated to provide personal data and the possible consequences if the data is not provided; and
- (l) information about the existence of automated decision-making, including profiling.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Individuals have the following rights with respect to their personal data:

- (a) Right to be informed;
- (b) Right of access;
- (c) Right to rectification;
- (d) Right to erasure;
- (e) Right to restriction of processing;
- (f) Right to data portability;
- (g) Right to object; and
- (h) Right not to be subject to a decision based solely on automated processing, including profiling.

Data controllers must facilitate the exercise of data subject rights and provide the data subject with information on action taken regarding a request without undue delay. All the above-mentioned rights may be restricted in situations enumerated by the LPDP if these restrictions do not affect the substance of fundamental rights and freedoms and if they are necessary and proportionate.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

- (a) Regarding advertising activities, the Advertising Law stipulates that prior consent is required in the case of direct advertising, ie, sending an advertisement message to a specific individual or otherwise individually identified person.
Consent given for this purpose can be revoked at any time, and the advertiser or transmitter of the advertisement message must enable this.
- (b) The issue of direct advertising is also further regulated by the Consumer Protection Law, which prohibits direct advertising via phone, fax, or email without the prior consent of the consumer, as well as for consumers who have registered their phone number in the registry of consumers who do not wish to receive calls and/or messages related to promotions and/or sales by phone.
On the other hand, when personal data is processed in this regard, provisions regarding the protection of personal data also apply.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The LPDP does not include specific provisions regulating the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers), so general privacy provisions apply.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

- (a) In cases where data processing is carried out on behalf of the controller by a processor, such processing must be governed by a contract or another legally binding act, which is concluded or adopted in written form, including electronic form. This act must bind the processor to the controller and regulate the subject and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, as well as the rights and obligations of the controller.
- (b) The relationship and responsibility for compliance with the obligations prescribed by the LPDP between two or more controllers that jointly determine the purpose and means of processing, ie, joint controllers, must be defined in a transparent manner.
Such responsibility must be regulated by an agreement between the joint controllers unless this responsibility is prescribed by a law applicable to the controllers. The agreement must designate a contact point for the data subject and regulate the relationship of each joint controller with the data subject. The essence of the agreement's provisions must be made available to the data subject.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Depending on the type of personal data that companies process, as well as the methods and actions of processing, the necessary measures that a company must undertake will vary. As a general rule, a

company adopts a privacy policy as an act that broadly regulates personal data protection. In addition to this and, depending on the entities with whom the company collaborates, it is necessary to conclude the agreements mentioned in question 6.2 and obtain the necessary consent for further processing.

However, if it is likely that a certain type of processing, particularly through the use of new technologies, and considering the nature, scope, circumstances, and purpose of the processing, will result in a high risk to the rights and freedoms of natural persons, the controller is required to conduct an impact assessment of the intended processing activities on personal data protection before commencing processing. If multiple similar processing activities may pose similar high risks to personal data protection, a joint assessment may be conducted. When conducting the impact assessment, the controller is obliged to seek the opinion of the data protection officer, if one has been appointed.

An impact assessment is mandatory in the following cases:

- (a) systematic and comprehensive assessments of the state and characteristics of a natural person carried out through automated processing of personal data, including profiling, which lead to decisions that significantly affect the legal position of the individual or similarly have a significant impact on them;
- (b) processing of special categories of personal data or personal data related to criminal convictions and offenses, on a large scale; and
- (c) systematic monitoring of publicly accessible areas on a large scale.

Such an impact assessment must at least include the following:

- a comprehensive description of the intended processing activities and the purpose of the processing, including a description of the legitimate interest of the controller, if applicable;
- an assessment of the necessity and proportionality of the processing activities in relation to the purposes of the processing;
- an assessment of the risks to the rights and freedoms of the data subjects; and
- a description of the measures intended to be taken in relation to the identified risks, including protection mechanisms, as well as technical, organizational, and personnel measures aimed at protecting personal data and ensuring compliance with the provisions of this law, taking into account the rights and legitimate interests of the data subjects and other individuals.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The main requirement for processing personal data for the purpose of sending direct marketing communications such as emails, mobile text messages or push notifications is informed consent of the data subject. The data subject must be informed on:

- (a) all aspects of marketing communications which involve processing of the data subject's personal data (eg, email address, telephone number etc);
- (b) the scope of the marketing communication; and
- (c) their right to revoke consent and on the means of revocation.

Pursuant to the Advertising Law, as well as the LPDP, consent once given can be revoked by the data subject at any time without meeting any special requirements. Revocation of consent leads to immediate cessation of data processing for this particular purpose, but does not, in any way, impact processing done before the moment of revocation of consent.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies is not explicitly regulated in the Serbian legal system; therefore, the general rules of the LPDP apply. This means, practically, that potential subjects of tracking technologies must give their consent for their use and be informed on all aspects of processing of their personal data via these tracking technologies.

For example, in terms of cookies on a particular website, visitors must be introduced, during their first visit to the site, to the site's cookie policy and their consent regarding the use of cookies in the way described in the policy must be given (usually by clicking 'I Agree' or 'Enable Cookies' on the cookie notice).

Visitors must also be made aware that they can disable cookies that they don't want to be active during their stay on the website at any time.

7.3 How are loyalty programs and promotions regulated under privacy law?

In accordance with the general rules of the LPDP, the company which is the organizer of a loyalty program, as the data controller, must obtain prior consent and notify all users of the program on all important aspects of processing of their personal data for this purpose.

This is usually done via the company's loyalty program privacy notice, which must contain all relevant information regarding personal data processing.

Regarding promotions, if personal data of consumers is involved in any way, prior consent or, in some cases, legitimate interest of the controller for its use is required, pursuant to the general rules of the LPDP.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing are not explicitly regulated by the Serbian legal system; therefore the general rules on personal data protection apply.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Behavioral advertising is not explicitly regulated by the Serbian legal system; therefore, the general rules of the LPDP apply.

As for targeted advertising (in the context of direct advertising, or marketing), the Advertising Law requires the prior consent of the targeted subject, which can be revoked at any time.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not regulated under the provisions of LPDP.

7.7 How is location-based advertising regulated under privacy law?

There are no specific provisions governing location-based advertising. However, location data is explicitly recognized as a typical category of personal data subject to LPDP.

7.8 How are data brokers defined and regulated under privacy law?

There are no particular rules that govern data brokers; therefore, the general rules on personal data protection apply.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors is not specifically regulated by the LPDP, but the issue of special protection of children and minors in advertising is addressed by the Advertising Law. In order to protect children and minors, it is stipulated that the advertising message must not:

- (a) depict a child or minor in a dangerous situation;
- (b) directly encourage children or minors to purchase goods or services or to ask their parents for them;
- (c) encourage children or minors to engage in behavior that may harm them;
- (d) directly encourage children or minors to purchase or lease goods or services, exploiting their inexperience and gullibility; or
- (e) abuse the special trust that children and minors place in their parents, teachers, or other individuals.

During a program intended for children or minors, only advertising messages and TV sales messages that are appropriate for their age may be broadcast. Additionally, during and at least ten minutes before or after the airing of a children's program or a program intended for minors, it is particularly prohibited to broadcast advertising messages and TV sales messages that recommend:

- alcoholic beverages;
- gambling games;
- ignition devices, flammable substances, and other dangerous materials that may endanger a child or minor;
- weight loss products, treatment procedures, establishments providing such services, medications, medical devices, and dietary supplements.

The law also includes other provisions aimed at protecting children and minors, seeking to ban advertising in schools, preschools, or other institutions intended for children or minors, unless it serves to protect the public interest and the interests of children or minors. Additionally, it seeks to limit the manner of advertising, such as prohibiting the advertising of alcoholic beverages to children and minors, either directly or indirectly, or through the depiction of children or minors in the context of alcohol consumption, all accompanied by a warning message indicating the prohibition of selling and serving alcoholic beverages to children or minors.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no particular rules that govern the use of artificial intelligence. On the other hand, the issue of automated decision-making and profiling is regulated by provisions of the LPDP, which stipulate that the data subject has the right not to be subject to a decision made solely on the basis of automated processing, including profiling, if the decision produces legal effects concerning that person or significantly affects their position.

However, this will not apply if the decision is:

- (a) necessary for the conclusion or performance of a contract between the data subject and the data controller;
- (b) based on law, if the law provides appropriate safeguards for the rights, freedoms, and legitimate interests of the data subject; or
- (c) based on the explicit consent of the data subject.

In these cases, the controller is required to implement appropriate measures to protect the rights, freedoms, and legitimate interests of the data subject, including, at least, the right to ensure the participation of the individual under the controller's supervision in the decision-making process, the right of the data subject to express their opinion regarding the decision, as well as the right of the data subject to challenge the decision before an authorized person within the controller's organization.

Such decisions cannot be based on personal data defined as special categories of personal data (see question 3.2), except in cases of a legally prescribed exception (eg, when the data subject has given explicit consent for processing for one or more purposes of processing), and appropriate measures are in place to protect the rights, freedoms, and legitimate interests of the data subject.

The LPDP prohibits the making of a decision solely based on automated processing carried out by competent authorities for special purposes, including profiling, if such a decision could result in harmful legal consequences for the data subject or significantly affect the position of that person, unless the decision is based on law and the law provides appropriate measures to protect the rights and freedoms of the data subject, including at least the right to ensure the participation of the individual under the controller's supervision in the decision-making process.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Data transfer under the LPDP is governed by a slightly different set of rules than those contained in the GDPR. Although most essential parts remain the same, there are some specific differences that need to be pointed out.

The transfer can be done in the following cases:

- (a) **Transfer based upon the adequate level of protection:** I.e., in cases where the transfer is made to one of the states or international organizations which are members of the EEA, or that are listed by the Serbian government as entities which provide an adequate level of data protection;
- (b) **Transfer based upon adequate measures for data protection:** If the transfer is not made to a country to which (a) applies, the controller and processor are responsible for providing adequate measures of data protection for that transfer. The stated obligation can be fulfilled in different ways, as stated by law (eg, a legally binding act between two authorities, standard contract clauses made by the Commissioner, binding corporate rules, code of conduct, etc);
- (c) **Transfer of data in special situations:** If it is not possible to fulfil the requirements of (a) or (b), the data transfer can be performed only in some specific cases (eg, the transfer is authorized by the data subject, the transfer is necessary for the execution of contract between the data subject and the controller, transfer is necessary for the protection of an important public interest prescribed by law, etc). This kind of data transfer obliges the controller to provide specific information to the data subject, and, in some cases, to inform the Commissioner about the data transfer;

- (d) **Transfer of data made by the competent authorities for specific purposes:** This kind of transfer is governed by its own specific rules. It is not, in detail, prescribed by the GDPR, but it is partially implemented into the LPDP from the EU Police Directive. A large number of important articles of the LPDP, including those regarding data transfer prescribe either exceptions to, exclusions from, or a completely new set of, rules governing the data transfer done by the competent authorities for specific purposes. The main problem is that, although 'data processing for specific purpose' is prescribed (ie, processing for the purpose of criminal investigations, public and national safety, prosecuting of criminals, etc), what is not precisely prescribed is which are the competent authorities that are authorized to perform that kind of processing, and therefore the transfer. For that reason, it is safe to say that the data transfer requirements and restrictions that are in force in cases of data processing and transfer by the competent authorities for specific purposes are different to those in force for other entities.

8.2 **Are there any additional considerations for personal data transfers (eg, privilege concerns)?**

The LPDP allows companies to pass so-called 'binding corporate rules' ('BCCs') which can apply instead of the general rules of the LPDP in situations when personal data is transferred between companies which are members of the same group or are members of the same multinational company.

The Commissioner will approve BCCs within 60 days from the date of application for their approval if they fulfil the following conditions:

- (a) they are legally binding, applicable to and enforced by each member of a multinational company or group of economic entities, including their employees;
- (b) they explicitly ensure the exercise of the rights of data subjects in connection with the processing of their data; and
- (c) they meet certain specified criteria.

The Commissioner may further regulate the way information is exchanged between controllers, processors and the Commissioner.

If all these conditions are fulfilled, the Commissioner will approve BCCs within 60 days from the date of application for their approval. However, if the data processing is undertaken by the competent authority, the rules referred to in this question will not apply.

9 **DATA SECURITY AND BREACH MANAGEMENT**

9.1 **How is data security regulated in Serbia? Are there minimum standards? Does this differ by sector or size of the entity?**

Data security is regulated by the LPDP, which prescribes that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, both the controller and processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures include, inter alia:

- (a) the pseudonymization and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The controller and processor must take steps to ensure that any natural person, acting under the authority of the controller or the processor, who has access to personal data does not process such data except on instructions from the controller or is required to do so by law. Furthermore, in assessing the appropriate level of security, the risks presented by processing, in particular the risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed, need to be taken in account.

In addition, associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of the national law regulating data protection, including application in respect of the measures aimed at ensuring security of processing.

9.2 **How are personal data breaches regulated in Serbia? What are the requirements for notification and response?**

If a data breach occurs, the law prescribes obligations for both controller and processor.

- (a) The processor is obliged to inform the controller without undue delay after becoming aware of such a breach.
- (b) The controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner. The controller has to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. In addition, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is obliged to communicate the personal data breach to the data subject without undue delay.

When assessing data breaches, the LPDP prescribes the imposition of administrative fines, which must, in each individual case, be effective, proportionate and dissuasive. Before being imposed, all relevant circumstance of the case must be taken into account, including the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage suffered by data subjects, etc.

10 **ENFORCEMENT AND PENALTIES**

10.1 **What penalties exist for non-compliance with privacy law?**

- (a) Under the LPDP, controllers and processors can be fined between RSD 5,000–2 million (approx €40–16,900) for violation of the rules concerning privacy and processing of personal data. Fines can also be levied on entrepreneurs, on responsible office holders and on other natural persons in certain cases.
- (b) The Law on Information Security also prescribes that a fine of RSD 50,000–2 million may be imposed on an ICT system operator of special significance (essential service provider, as defined in NIS Directive) for a misdemeanor related to personal data, among other things, and a responsible person within the ICT system operator of special importance may also be fined.

- (c) Finally, the Serbian Criminal Code prescribes fines, as well as imprisonment for up to 3 years for criminal acts related to violation of rules regarding personal information, such as the unauthorized disclosure of a secret, breach of secrecy of letters and other items, unauthorized wiretapping and recording, unauthorized photography, unauthorized publication and display of other people's files, portraits and footage and unauthorized collection of personal information.

10.2 Do consumers have a private right of action? What remedies are available to them?

In cases where a data breach has taken place, the law provides various legal remedies for a data subject:

- (a) **Right to lodge a complaint with the Commissioner:** A data subject has a right to lodge a complaint with the Commissioner, if they consider that the processing of personal data relating to them infringes the LPDP. Lodging a complaint with the Commissioner does not influence the data subject's right to initiate court proceedings. The Commissioner will inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy against the Commissioner's decision.
- (b) **Right to an effective judicial remedy against a Commissioner's decision:** Every natural or legal person, including the data subject, processor and controller, has the right to an effective judicial remedy against a legally binding decision of the Commissioner concerning them, by filing a lawsuit with the Administrative Court within 30 days from the day of the receipt of the Commissioner's decision. A data subject may also initiate administrative court proceedings in cases when the Commissioner does not render a decision within 60 days from the day of the receipt of the complaint or fails to inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy against Commissioner's decision.
- (c) **Right to initiate court proceedings:** A data subject has a right to initiate court proceedings before competent court if they consider that the controller or processor has infringed their rights when processing their personal data. Initiating court proceedings does not influence the data subject's right to initiate other administrative or judicial proceedings. In the lawsuit, the data subject may request the court to oblige the defendant to:
 - (i) give information that data subject is entitled to know,
 - (ii) rectify or erase data,
 - (iii) restrict processing,
 - (iv) provide data in a structured, commonly used and machine-readable format,
 - (v) transfer data to another controller or
 - (vi) stop data processing.

In addition, a data subject may apply to court to determine that a decision concerning them was made contrary to provisions regulating decisions based solely on automated processing, including profiling.
- (d) **Right to compensation:** Any person who has suffered material or non-material damage as a result of an infringement of the LPDP has the right to receive compensation from the controller or processor for the damage suffered. A controller is liable for such damage, while a processor is liable only where it has not complied with obligations of the law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. The controller or processor may be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Although there is activity from enforcers, no decision has been published that has significantly influenced practice or that could be useful regarding issues of alleged privacy non-compliance involving advertising.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Serbia?

There are no cultural considerations that impact privacy law or enforcement in Serbia.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

In its most recent annual report to the National Parliament in 2023, the Commissioner, in an effort to improve personal data protection in Serbia, submitted proposals to the National Assembly and the Government, highlighting the necessity of adopting amendments to the LPDP.

The report also emphasized that parliamentary committees and expert services should carefully consider the Commissioner’s opinions on how proposed laws may affect the right to personal data protection. It further called for timely and full institutional support for the Commissioner as an independent state body in carrying out its mandate.

Moreover, the necessity of adopting laws with provisions on personal data processing that align with the LPDP was highlighted.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

- (a) The LPDP, which is based heavily on the provisions of the EU’s GDPR, prescribes much stricter terms and requirements under which personal data can be processed. The severity of sanctions and penalties for unlawful personal data processing has also been increased.
- (b) Companies which are based in Serbia or are based abroad but conduct processing of personal data in Serbia in any way should conduct their processing on a lawful basis and, in general, be as transparent as possible towards the data subjects and authorities regarding personal data processing.
- (c) Data subjects should also be regularly notified on any changes in processing of their personal data and be given full freedom whenever possible to decide what happens to their personal data and how it is processed, unless processing of certain types of data in a certain way is required by law or at the request of a competent authority.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

In the privacy landscape, there have been no significant changes, meaning there have been no amendments to the LPDP since the law came into force in 2018, despite calls for amendments.

In the area of personal data protection, the only major development in recent years has been the adoption of the LPDP in 2018, which at the time offered fresh updates and solutions to existing problems not covered by the previous Law and brought the Serbian legal system one step closer to harmonization with the legal system of the European Union.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The main challenge that companies face currently due to the adoption and application of the GDPR and the application of the LPDP in Serbia is the harmonization of companies' internal documentation, acts and procedures.

Given the fact that the LPDP, which is heavily based on the GDPR, prescribes, in detail, numerous new requirements, obligations and terms that must be met in regards to processing of personal data, mechanisms that are yet to be implemented and tested in practice, and much harsher fines, all companies that undertake processing of personal data in any way must rush to make amendments to their internal documentation, including contracts where these concern personal data processing.

Depending on the scope of processing of personal data undertaken by a particular company, this can be a very time-consuming and expensive process, and even confusing at times, given the magnitude of changes which have been brought in at once.

Finally, taking into account that the LPDP was only adopted in 2018, the lack of Commissioner's and judicial legal practice also represents a serious challenge in the new privacy landscape that companies must navigate. Only with further rulings and decisions in the application of the LPDP will companies be able to conduct their business in line with data protection rules and procedures with greater certainty.

12.3 What do you envision the privacy landscape will look like in five years?

The Serbian privacy landscape in 5 years' time will largely depend on the process of Serbia's accession to the European Union. In addition, due to rapid growth of the 'information market' and the rise of new technologies, it is reasonable to expect that the existing LPDP will have to be amended and supplemented with bylaws in order to stay relevant and in touch with the coming times and developments.

Furthermore, in order to ensure a greater degree of data protection, it can be expected that the capacity of the Commissioner to monitor and enforce the application of existing data protection rules and procedures will be bolstered and enhanced in the coming period.

 SINGAPORE 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Singapore.

There is no single, overarching legislation in Singapore which governs privacy regulation as a whole. Be that as it may, there are laws which regulate, inter alia, access to and processing of personal data, in addition to sector-specific legislation. In particular:

- (a) the Personal Data Protection Act 2012 (2020 Revised Edition) ('PDPA'); and
- (b) the Spam Control Act 2007 (2020 Revised Edition) ('SCA').

1.2 What are the primary laws regulating privacy in Singapore? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

See response to question 1.1.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation plays an important role in privacy regulation, particularly for advertising practices in Singapore, by complementing legal frameworks such as the PDPA and SCA. Through codes such as the Singapore Code of Advertising Practice, organizations in advertising voluntarily adhere to ethical standards that promote transparency of advertisements and protect consumer interests. The Advertising Standards Authority of Singapore enforces these ethical guidelines, promoting best practices for data collection, use, and processing in advertising. Self-regulation enables organizations' advertising practices to go beyond mere compliance, aligning with both privacy laws and ethical advertising standards.

1.4 How is privacy law enforced in Singapore? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

- (a) The Judiciary, through the Supreme Court of Singapore as well as the State Courts of Singapore, provides recourse with regards to privacy-related matters to common law remedies, such as breach of confidence. At the outset, a claim may be filed in court by an affected party, and the court will then determine whether there has been a breach of the law.
- (b) Another instance where the courts are involved is to adjudicate on sector-specific breaches of privacy-related legislation such as the Official Secrets Act and Banking Act. In such cases, the complaint is usually made by the Attorney-General's Chambers, though private prosecution also be brought in certain circumstances.
- (c) In certain industries, there are self-regulatory bodies that play an important role in enforcing privacy laws. Examples of such bodies include the Monetary Authority of Singapore and Advertising Standards Authority of Singapore. These bodies regulate compliance with general privacy laws, including the PDPA, and sector-specific Codes of Practice.
- (d) The PDPA confers various powers on the Personal Data Protection Commission ('PDPC') to enforce provisions of the PDPA. The PDPC is part of the Infocomm Media Development Authority. These powers may generally be categorized as follows:
 - (i) **Investigation:** The PDPC is empowered to determine whether an organization is complying with the PDPA, and to direct an organization that is not complying to take the appropriate corrective actions to ensure compliance.

- (ii) **Review:** The PDPC is empowered to review an organization's response to a request made by an individual under the PDPA. The PDPC can either confirm the organization's reply or direct the organization to take certain corrective actions in relation to the request.
- (iii) **Alternative dispute resolution:** These powers generally relate to the manner in which the PDPC facilitates the resolution of disputes between complainants and organizations through methods such as mediation or other modes of alternative dispute resolution, promoting efficient settlement outside of the courts.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Singapore?

The PDPA applies primarily to organizations that collect, use, or disclose personal data in the course of commercial activities in Singapore. The PDPA does not apply to the following:

- (a) any individual acting in a personal or domestic capacity;
- (b) any employee acting in the course of their employment with an organization;
- (c) any public agency or an organization in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data; or
- (d) any other organizations or personal data, or classes of organizations or personal data, prescribed for the purposes of this provision.

Organizations which are data intermediaries are partially excluded from obligations under the PDPA. Further, business contact information is not covered under the provisions of the PDPA.

2.2 Does privacy law in Singapore apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The data protection obligations under the PDPA apply to all organizations which collect, use or disclose personal data in Singapore, irrespective of whether or not they are incorporated or formed under Singapore law, and whether or not they are resident or have an office or place of business in Singapore.

In addition, the Do-Not-Call requirements and obligations under the PDPA apply to all organizations which send marketing messages to a Singapore telephone number.

See also the transfer obligation (discussed at question 4.1).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Singapore?

The PDPA defines 'personal data' as 'data, whether true or not, about an individual who can be identified:

- (a) from that data; or
- (b) from that data and other information to which the organization has or is likely to have access'.

The term 'personal data' is not intended to be narrowly construed and may cover different types of data about an individual and from which an individual can be identified, regardless of such data being true or false or whether the data exists in electronic or other form.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

While there are no objective criteria to determining sensitivity, there is support for harm-based analysis whereby the greater the potential for harm, the more sensitive the data are considered to be.

One instance in which the sensitivity of data has been considered is in relation to the obligations on organizations following a data breach (see further question 9.2). In circumstances where it is determined that a breach is likely to result in significant harm to affected individuals, organizations are required to notify the individuals concerned. To this end, the Personal Data Protections (Notification of Data Breaches) Regulations 2021 provide classes of personal data that are deemed to result in significant harm to affected individuals if a breach occurs. These include:

- (a) an individual's full name or alias or full national identification number;
- in combination with any of the following personal data (or classes of personal data):
- (b) financial information that is not publicly disclosed, such as an individual's salary, net worth or creditworthiness;
 - (c) identification of vulnerable individuals: this includes a child or young person who is or has been the subject of any investigation under the Children's and Young Person's Act, or an adult who has been or is the subject of any investigation, assessment or treatment under the Vulnerable Adults Act;
 - (d) the name or address of any woman who has been subjected to a sexual crime;
 - (e) life, accident and health insurance information that is not publicly disclosed, such as the terms and conditions of such policies or the premium payable by the policy owner;
 - (f) specific medical information, such as the assessment, diagnosis, treatment, prevention or alleviation of any sexual transmitted disease; and
 - (g) information related to adoption matters, such as the identity of the biological parents of an adopted child.

In cases of such breaches, the organization will be required to notify the data breach to the affected individuals and the Commission. The notification to the PDPC must be made as soon as practicable, but no later than three calendar days after the breach is discovered. Notification to the affected individuals should also be as soon as practicable, or at the same time as or after notifying the Commission.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Data that has been truly anonymized, whereby identifying information has been removed so that the remaining data cannot be used to identify any particular individual, whether on its own or in combination with other information, is no longer considered personal data for the purposes of the PDPA. The same is true of pseudonymized, or de-identified data; although pseudonymized or de-identified data, which can potentially be re-identified (eg, by linking to other datasets, even if the process is difficult), may still be considered personal data if it can be linked back to an individual, even if such link is indirect.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Under the PDPA, the main obligations with which an ‘organization’ (which includes any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognized under the law of Singapore, and whether or not resident, or having an office or a place of business, in Singapore) (including, but not limited to, advertisers) will need to comply have been identified by the PDPC in their Advisory Guidelines on Key Concepts in the Personal Data Protection Act (the ‘Key Concepts Guidelines’). They are as follows:

- (a) **The Consent Obligation:** Parties may collect, use or disclose personal data for purposes for which an individual has given their consent, whether express or implied. Individuals should also be allowed to withdraw such consent, upon reasonable notice. Upon withdrawal of consent to the collection, use or disclosure of an individual’s personal data for any purpose, parties must cease such collection, use or disclosure of the personal data for such purpose.
- (b) **The Notification Obligation:** The individual must be notified of the purposes for the collection, use or disclosure of the personal data on or before such collection, use or disclosure.
- (c) **The Purpose Obligation:** Parties may collect, use or disclose personal data only for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent, and not for any other purposes. Parties may not, as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of their personal data beyond what is reasonable in order to provide that product or service.
- (d) **The Access and Correction Obligations:** Parties must as soon as reasonably possible upon request:
 - (i) provide an individual with their personal data in the possession, or under the control, of the organization, and information about the ways in which the personal data may have been used or disclosed during the past year; and
 - (ii) correct any error or omission in an individual’s personal data that is in the possession or under the control of the organization.
- (e) **The Accuracy Obligation:** Parties must make reasonable efforts to ensure that personal data collected by or on behalf of the organization is accurate and complete if the personal data is likely to be used by the organization to make a decision that affects the individual concerned, or to be disclosed by the organization to another organization.
- (f) **The Protection Obligation:** Parties must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying modification or disposal, or similar risks; or the loss of any storage medium or device on which the personal data is stored.
- (g) **The Retention Limitation Obligation:** Parties must cease to retain documents containing personal data, or remove the means by which personal data can be associated with particular individuals, as soon as it is reasonable to assume that:
 - (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and
 - (ii) retention is no longer necessary for legal or business purposes.

- (h) **The Transfer Limitation Obligation:** Parties are prohibited from transferring personal data to a country or territory outside Singapore except in accordance with the requirements under the PDPA.
- (i) **The Data Breach Notification Obligation:** Parties must assess whether a data breach is notifiable, and notify the affected individuals and/or the PDPC where a breach is assessed to result in or is likely to result in significant harm to an affected individual or is likely to be of a significant scale.
- (j) **The Accountability Obligation:** Parties must develop and implement the necessary policies and procedures in order to meet their obligations under the PDPA, as well as develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. Additionally, parties must make information about their policies, complaints process and procedures available on request

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Every organization is required to comply with the provisions contained in the PDPA. Be that as it may, a data intermediary that processes personal data on behalf of, and for the purposes of, another organization will only be subject to those provisions which relate to the protection, retention and notification to organizations of data breaches of personal data, but not any of the other data protection provisions. Such a data intermediary will still remain responsible for complying with all PDPA obligations for any other activities.

An organization that uses a data intermediary to process personal data on its behalf has the same obligations under the PDPA as if the personal data were processed by the organization itself. As such, when engaging a data intermediary, an organization must clearly define the scope of work to be carried out on its behalf and for its purposes. Where a data breach is identified by the data intermediary, it is the responsibility of the data intermediary to notify the organization. However, the liability for such breach remains with the organization, as it is ultimately responsible for the personal data processed on its behalf.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See question 4.1, specifically the Consent Obligation under the PDPA, which outlines these grounds and emphasizes that organizations must inform individuals about the purposes of data collection, use, and disclosure, and ensure the lawful basis for processing is established.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the PDPA, organizations must include specific information in their privacy notices to ensure transparency and compliance:

- (a) the purpose for which the personal data will be collected, used, or disclosed (targeted advertising, behavioral advertising, or profiling) (see question 4.1);
- (b) the types of personal data they collect for advertising purposes;

- (c) whether the personal data will be shared with third parties, such as advertising partners, analytics providers, or social media platforms; and
- (d) it must inform individuals that they have the right to withdraw their consent to the processing of their personal data for advertising purposes at any time and should provide instructions on how individuals can withdraw their consent. To this end, the privacy notice should provide contact details for the organization, particularly if individuals have questions about the processing of their personal data or wish to exercise their rights.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

The PDPA recognizes the rights of individuals to protect their personal data, including, but not limited to, the right of access and correct their data (see question 4.1).

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the PDPA, companies must obtain consent or provide opt-out options for advertising activities in specific circumstances:

- (a) **Consent:** Consent is required for the collection, use, or disclosure of personal data for advertising activities (including direct marketing). When personal data is used to send direct marketing communications, such as advertising via email, SMS, phone calls, or other forms of direct communication, consent is needed. See question 7.1 as to the Do Not Call Registry.
- (b) **Opt-out options:** Organizations must allow individuals to opt-out of receiving marketing communications at any time and this can be done by providing clear instructions in every marketing communication (eg, an unsubscribe link in emails or an option to opt-out of SMS marketing). The company must stop sending marketing communications within 30 days after the opt-out is exercised.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Under the PDPA, the organization collecting or controlling the personal data (ie, the data controller) remains responsible for ensuring that personal data is handled in compliance with the PDPA, even when third parties or vendors are involved. To this end, organizations are required to enter into legally binding contracts with vendors and third parties to ensure that personal data is processed in compliance with the PDPA's data protection principles, such as the Purpose Limitation and Accuracy obligations (see question 4.1). Vendors must take appropriate measures to ensure the security of the personal data they process pursuant to these principles.

When personal data is used for targeted advertising through vendors and third parties, organizations must obtain the individual's explicit consent for the collection, use, and disclosure of their personal data for such purposes.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The contractual obligations must ensure compliance with PDPA's data protection principles (see question 4.1). The contract should also contain a confidentiality clause ensuring that the third party or vendor keeps the personal data confidential and does not disclose it to unauthorized parties.

It is important for the contract to specify the third party's obligation to notify the data controller of any data breaches or security incidents involving personal data, as required under the PDPA, and that such notification should be made without undue delay, ideally within 72 hours of becoming aware of the breach.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Most importantly, organizations should ensure that their privacy practices comply with the various obligations under the PDPA (see question 4.1).

If an organization is engaging third party data vendors (eg, advertising agencies) that will access to personal data, the organization should conduct due diligence by ensuring that vendors comply with the PDPA and provide adequate data protection safeguards.

Additionally, organizations should appoint a data protection officer ('DPO') to oversee their data protection practices, ensure compliance with the PDPA, and serve as a point of contact for privacy-related matters. Regular training should be conducted for the DPO and other relevant staff to ensure they are up to date with privacy laws and best practices.

The carrying out of impact assessments is another due diligence measure which organizations should adopt. Impact assessments entail identifying, assessing and addressing personal data protection risks based on the organization's functions, needs and processes. They can be conducted when creating new systems/processes involving handling of personal data or when changing way that existing systems/processes handle personal data (eg, new database/portal). Impact assessments ideally identify how data flows through the system/process so as to identify risks and enable implementation of security measures addressing risks.

Currently, impact assessments are only statutorily mandated under the PDPA for deemed consent by notification and for the legitimate interest exception. The assessment must identify any adverse effect the proposed collection, use/disclosure of the individual's personal data is likely to have on the individual, and must identify and reasonable measures that may be implemented to eliminate the adverse effect, reduce the likelihood that the adverse effect will occur, or mitigate the adverse effect.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The PDPC maintains a Do Not Call Registry which allows individual subscribers of Singapore telephone numbers to opt out of marketing calls, SMSs and faxes to their numbers by registering in one or more of the three registers (ie, the No Voice Call Register, the No Text Message Register and the No Fax Message Register). Generally, before sending a marketing call, SMS/MMS or fax to a Singapore

telephone number (where the subscriber is an individual), an organization must apply to the Do Not Call Registry to confirm whether the number is listed in the Register, unless it has obtained prior clear and unambiguous consent from the subscriber of the number.

Business-to-business ('B2B') marketing calls, SMSs/MMS, and fax messages are not subject to the Register. Hence, it is permissible for parties to send B2B SMS/MMS messages without checking the Register, provided the subscriber of the number is a corporate entity and not an individual. However, since subscribers enlisted with the telcos are typically individuals, rather than the corporate entities which employ them, ascertaining whether the number to which an SMS will be sent belongs to an individual or a corporate entity may be difficult. Hence, the safer and easier alternative will be to check the Register and/or obtain unambiguous consent from the individual, prior to sending a marketing SMS.

If organizations have an ongoing relationship with a subscriber of a Singapore telephone number (and have obtained clear and unambiguous consent), they may send marketing SMSs, calls or faxes to the number without checking the Register. Each SMS sent under this exemption must contain an opt-out mechanism that the subscriber can use to opt out from receiving such an SMS. If a subscriber opts out, the organization can no longer rely on the exemption and must cease sending marketing SMSs to that number, within 30 days.

The Do-Not-Call framework under the PDPA covers only telephone calls, SMS/MMS, and faxes. It does not include emails and mail delivered by post. Therefore, to circumvent the onerous requirements of the PDPA, organizations may consider using emails instead of SMSs (although this may be slightly less effective from the marketing perspective). However, before sending marketing emails, organizations must comply with the requirements set out in the SCA, which regulates the sending of unsolicited commercial electronic messages in bulk. The requirements of the SCA can be regarded as less onerous than those under the PDPA.

The SCA stipulates that the following requirements for sending marketing emails:

- (a) the subject line must not be false or misleading regarding content of the message;
- (b) the letters '<ADV>' should appear before the subject line (or, if there is no subject line, at the start of the message) to clearly identify the message as an advertisement;
- (c) the header information must not be false or misleading; and
- (d) an accurate and functional contact email address or phone number must be provided for the sender.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The PDPA also applies to the collection, use, or disclosure of personal data through cookies and other tracking technologies. The Advisory Guidelines on the Personal Data Protection Act for Selected Topics ('Selected Topics Guidelines'), published by the PDPC, provide the following:

- (a) the obligation to obtain the individual's consent for the collection of their personal data lies with the organization that is collecting such personal data, whether directly or through its data intermediaries; and
- (b) where an organization operates a website which allows a third party to collect personal data, and the website operator itself is not collecting the personal data, the obligation is on the third-party organization to obtain the consent required to collect such personal data.

7.3 How are loyalty programs and promotions regulated under privacy law?

The general principles enunciated in the PDPA apply with equal effect to loyalty programs and promotions.

7.4 How is social media and influencer marketing regulated under privacy law?

The Selected Topics Guidelines provide the following guidance: The PDPA does not require organizations to obtain the consent of the individual when collecting personal data that is publicly available. Examples of publicly available sources include newspapers, telephone directories, and websites containing content which is generally accessible to the public. For social networking platforms where data is publicly available, the PDPA does not prohibit organizations from collecting personal data about an individual without their consent.

See question 4.1 ‘The Consent Obligation’ for further explanation of the ‘publicly available data’ exception.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

The PDPA also applies to targeted advertising and behavioral advertising. When these types of advertising involve the collection, disclosure or use of personal data, the individual’s consent must be obtained before their data is used for such purposes.

Contextual advertising, in contrast to targeted advertising, delivers advertisements based on the content of the website or application being viewed rather than on personal data. Since contextual advertising does not rely on personal data, but rather on the context in which the user is interacting with content, it generally does not require the same level of scrutiny under the PDPA as targeted advertising. As long as no personal data is being collected, used, or disclosed for the purpose of delivering the advertisement, the PDPA may not apply in the same way. However, if any personal data is collected indirectly (such as through cookies or device identifiers), consent would still be required under the PDPA.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution, which refers to the process of combining data from multiple sources (both online and offline) to create a more complete profile of an individual, and clean room technologies, which refers to a secure environment where multiple organizations or entities can aggregate and analyze data without exposing raw personal data to any party, often involve the use of personal data for various purposes, including targeted advertising, data analytics, and audience segmentation. Both technologies will need to comply with the obligations under the PDPA (see question 4.1).

Additionally, with respect to data clean rooms, to minimize re-identification of individuals, the use of data anonymization or pseudonymization techniques is important. This ensures that the data shared within the clean room cannot be traced back to individuals. If third-parties are involved, organizations must ensure that these third parties are compliant with the PDPA.

For both technologies, organizations may need to conduct data protection impact assessments. Organizations must also ensure compliance with the SCA and the Do Not Call Registry provisions.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is regulated under the PDPA and needs to comply with the various obligations imposed by that Act (see question 4.1) as it involves the collection of personal data that can identify or track individuals. Personal data can include location data (eg, GPS data, Wi-Fi signals, and other geolocation information) that reveals information about an individual's physical movements, habits, and preferences. In particular, one of the most important requirements would be obtaining consent from the individual whose location data is being collected and used. Organizations involved in location-based advertising must include clear information in their privacy notices regarding the collection of location data, such as the type of data being collected, how the data will be used and if there will be any third-party sharing of the data. Additionally, location-based advertising may be subject to other regulatory requirements such as the SCA and Do Not Call Registry.

7.8 How are data brokers defined and regulated under privacy law?

While data brokers are not explicitly defined under the PDPA, they are generally understood as entities who collect, process, and sell or trade personal data, often aggregating data from multiple sources. The general principles outlined in the PDPA apply equally to data brokers (see question 4.1). Data brokers are subject to the same obligations regarding the collection, use, and disclosure of personal data as other organizations under the PDPA. Additionally, data brokers may be subject to other regulatory requirements such as the SCA and Do Not Call Registry. Data brokers may be regulated by self-regulatory mechanisms or industry codes of practice.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors is regulated under the PDPA which governs the collection, use, and disclosure of personal data (see question 4.1). Given the vulnerability of children and minors, the collection and processing of personal data for this group should be subject to stricter safeguards.

For minors less than 13 years of age, the Selected Topics Guidelines provides that organizations are to obtain consent from an individual who can legally give consent on behalf of the minor (eg, parent/guardian).

In the case of a minor who is above 13 years, the general rule would be that the minor has sufficient understanding to validly consent on their own behalf and the minor would be deemed to have consented if they voluntarily provide their personal data for that purpose (and it is reasonable that the individual would voluntarily provide the data). In assessing voluntariness, the minor's understanding of the purpose for which the personal data is provided and the effect of giving the data for that purpose and whether undue influence on minor with respect to providing the data.

Organizations should also consider taking extra steps to verify the accuracy of personal data about a minor, especially where such inaccuracy may have severe consequences for the minor.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Privacy laws, particularly the PDPA, regulate profiling, artificial intelligence ('AI'), and automated decision-making technology used for advertising purposes by requiring consent, transparency, and ensuring the fair use of personal data. See question 4.1.

As AI technologies evolve, regulatory frameworks may further address the complexities of automated decision-making in advertising, aiming to balance innovation with the protection of individuals' privacy rights.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The PDPA limits the ability of an organization to transfer personal data outside Singapore. Specifically, an organization must not transfer any personal data to a country or territory outside Singapore, except in accordance with the requirements prescribed under the PDPA. These requirements ensure that organizations provide a level of protection to personal data so transferred that is comparable to the protection afforded under the PDPA.

An organization may transfer personal data overseas if it has taken appropriate steps to ensure compliance with the data protection provisions in respect of the transferred personal data. This includes ensuring that the recipient, in the destination country or territory, is bound by legally enforceable obligations to provide a comparable level of protection to the personal data being transferred. If the recipient country is deemed adequate by the PDPC, the transfer may proceed without additional safeguards. The PDPA does not explicitly list specific countries where data transfers are prohibited. However, the PDPC may designate countries that do not offer an adequate level of protection, which would require organizations to adopt safeguards such as Standard Contractual Clauses ('SCC') that bind the recipient of the personal data to provide the necessary level of protection.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Companies may need to consider other legal and regulatory obligations that could affect data transfers, such as confidentiality, legal privilege, and contractual requirements within group companies.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Singapore? Are there minimum standards? Does this differ by sector or size of the entity?

The PDPA requires an organization to make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks and the loss of any storage medium or device on which personal data is stored. Indeed, the PDPC has recognized that there is no 'one size fits all' solution for organizations to comply with this obligation. Each organization should consider adopting security arrangements that are reasonable and appropriate in the circumstances, bearing in mind the nature of the personal data, the form in which the personal data has been collected (ie, whether physical or electronic) and the possible impact to the individual concerned if an unauthorized person obtained, modified and/or disposed of the personal data.

In practice, organizations are expected to:

- (a) design and organize their security arrangements to fit the nature of the personal data held by them and the possible harm that might result from a security breach;
- (b) identify reliable and well-trained personnel responsible for ensuring information security;
- (c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- (d) be prepared and able to respond to information security breaches promptly and effectively.

It may be useful for organizations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In so doing, the following factors should be considered:

- (i) the size of the organization and the amount and type of personal data in the organization's possession and control;
- (ii) who, within the organization, has access to the personal data; and
- (iii) whether the personal data is/will be held or used by a third party on behalf of the organization.

Large organizations, especially those handling large volumes of personal data, would be expected to have more comprehensive data security frameworks. Large organizations may also be expected to implement specific measures in line with international standards, especially if they are dealing with cross-border data transfers. Smaller and medium enterprises may face fewer regulatory requirements in terms of reporting and handling complex data security matters, but would still need to meet the minimum standards outlined in the PDPA.

9.2 **How are personal data breaches regulated in Singapore? What are the requirements for notification and response?**

Requirements as to mandatory data breach notification were added to the PDPA on February 1, 2021. Organizations are expected to take the following steps in cases of data breach:

- (a) contain the data breach to prevent further compromise of personal data;
- (b) assess the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals. Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organization proceeds to implement full remedial action;
- (c) report the data breach to the PDPC and/or affected individuals, if necessary; and
- (d) evaluate the organization's response to the data breach incident and consider actions which could be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

The PDPC advises organizations to report data breaches to the PDPC within 72 hours where the breach is either likely to result in significant harm or impact to individuals, or if it is of 'significant scale'. Further, organizations are advised to assess whether a potential breach meets this reporting threshold promptly, and no later than 30 days from learning of a potential data breach.

The PDPC may, if satisfied that an organization has contravened its PDPA obligations, give directions to the organization to ensure compliance and, in some instances, impose a financial penalty of up to S\$1 million.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The Guide on Active Enforcement published by the PDPC provides the following guidance:

- (a) As a matter of enforcement policy, the PDPC's approach is first to consider the nature of the breach and whether directions without financial penalties are effective in remedying the breach. Financial penalties are intended to act as a form of sanction and deterrence against non-compliance when directions alone do not sufficiently reflect the seriousness of the breach. In considering whether an organization should be directed to pay a financial penalty, the PDPC will take into account the seriousness of the breach. Generally, financial penalties are reserved only for breaches which the PDPC views as particularly serious in nature.
In assessing the seriousness of the breach, the PDPC considers a number of factors, including but not limited to, the following:
 - (i) impact of the organization's breach on affected individuals;
 - (ii) whether the organization had acted deliberately or willfully;
 - (iii) whether the organization knew or ought to have known about the risk of a serious contravention and failed to take reasonable steps to prevent it;
 - (iv) extent of non-compliance with the PDPA obligations that the organization had failed to discharge;
 - (v) number of individuals whose personal data was compromised or put at risks as a result of the breach;
 - (vi) whether the organization appointed a data protection officer ('DPO') or equivalent to ensure accountability with the PDPA;
 - (vii) types of personal data that were compromised or put at risk as a result of the breach; and
 - (viii) whether the organization had previously been found to have similarly breached the PDPA.
- (b) The PDPC determines each case based on its own merits and circumstances. However, the PDPC adopts an objective approach to assess the seriousness of a breach of the data protection provisions of the PDPA, by considering how a reasonable organization should behave in a particular situation. Where a financial penalty is warranted, the PDPC adopts the following principles to determine the amount:
 - (i) the amount should be proportionate to the seriousness of the breach;
 - (ii) the amount should provide sufficient deterrence against future or continued non-compliance by the organization and others;
 - (iii) the amount should take into account aggravating and mitigating factors, namely:
 - cooperativeness of the organization in the course of investigations;
 - whether remedial action(s) were implemented;
 - whether there was voluntary notification of the data breach;
 - whether the organization had engaged with the affected individuals in a meaningful manner and had voluntarily offered a remedy that the individuals accepted; and
 - whether the organization admitted liability for the data breach.

Currently the financial penalty for organizations is capped at S\$1 million or 10% of an organization's annual turnover in Singapore (whichever is higher), while for individuals it is capped at S\$200,000. Further, individuals may be criminally liable to a fine of up to S\$5,000 or an imprisonment term of up to two years if they are found to have egregiously mishandled personal data.

10.2 Do consumers have a private right of action? What remedies are available to them?

The PDPA provides individuals with the right to commence a private action against an organization where that individual has suffered loss or damage as a direct result of the organization's non-compliance with the data protection provisions under the PDPA, subject to certain limitations. However, this right to commence a private action can only be exercised after the PDPC has issued a decision regarding the contravention, and the decision has become final, after all avenues of appeal have been exhausted.

The court may grant such relief as it thinks fit including, but not limited to, an injunction or damages.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The PDPC is the primary enforcer of privacy-related matters under the PDPA. The PDPC is responsible for ensuring that organizations comply with the data protection obligations set out in the PDPA, including those related to advertising, personal data collection, use, disclosure, and processing.

The PDPC has been active in investigating and taking enforcement action against organizations for violations of the PDPA including issuing financial penalties, directions for corrective action, and advisories aimed at ensuring compliance with the law.

One example of enforcement action would be that which took place in 2021, when the PDPC investigated Singtel, one of Singapore's leading telecommunications companies, for the leak of personal data, including the names, addresses, and telephone numbers, of about 129,000 customers. The PDPC issued a financial penalty of S\$9,000 against Singtel for failing to comply with the PDPA's data protection and security obligations, as it did not implement reasonable security arrangements to prevent the unauthorized disclosure of personal data.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Singapore?

Singapore has rapidly embraced technological innovation, with a government-led Smart Nation initiative pushing for the use of technology in every aspect of life, including in healthcare, transportation, and financial services. The rapid adoption of digital technologies raises concerns about data security and privacy, particularly with the increased use of artificial intelligence, big data analytics, and cloud computing. Enforcement may need to balance the need for innovation and the use of personal data with the protection of individuals' privacy.

Singaporeans have traditionally placed less emphasis on privacy compared to some societies. However, as digitalization increases, so does awareness of the risks associated with data breaches, cyberattacks, and misuse of personal data.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

A change that has yet to come into effect is the introduction of data portability. This obligation will allow individuals to request a copy of their personal data be transmitted in a commonly used, machine-readable, format to another organization which would enable easier transitions for consumers between services providers.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

- (a) It is imperative for organizations to develop and implement comprehensive data protection policies and practices. These include processes to receive and respond to complaints that may arise with respect to the application of the PDPA and provide staff with training to execute these practices.
- (b) The PDPA now requires organizations to appoint a DPO, who is responsible for ensuring that the organization complies with the PDPA.
- (c) Carry out periodic audits.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, the privacy landscape in Singapore has seen several key changes, driven by both global trends and local developments, which have been prompted by increased digitalization, evolving consumer expectations, and a stronger emphasis on protecting personal data in an interconnected world.

With the advancement in technology, more sensors that collect biometric data are being used and deployed in commercial security applications such as security cameras, closed circuit TVs for security monitoring, facial and fingerprint recognition systems. The collection of such personal data would fall within the ambit of the legitimate interests exception recognized by the PDPA wherein organizations may collect, use or disclose personal data. In these cases, the organizations’ legitimate interest in relation to the personal data (ie, monitoring or investigations for security purposes) outweigh the adverse effect on the individual. The legitimate interests exception would generally apply for security cameras in areas not open to the public whereas for areas generally accessible to public the publicly available data exception would be more relevant. It is good practice to put up notices disclosing that the area is under surveillance and whether recording also takes place.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The law often struggles to keep pace with the rapid advancement of technology. This is especially true for organizations that must navigate evolving technologies—such as artificial intelligence, big data, and the Internet of Things whilst balancing the obligations set out in existing privacy legislation. Moreover, with the increasing reliance on cloud computing and cross-border data flows, companies face increased complexities in ensuring compliance with both local and international data protection standards.

The PDPC has done a commendable job in educating all stakeholders, and disseminating guidance and information on how to comply with the PDPA and the evolving regulatory landscape.

12.3 What do you envision the privacy landscape will look like in five years?

The Singapore regime has gradually shifted from a purely compliance-based model to one that emphasizes accountability for both organizations and individuals regarding personal data protection. Recent mandates, such as those requiring risk assessments and data breach notifications, indicate Singapore's clear move towards a more proactive, accountability-driven approach to privacy.

The COVID-19 pandemic has accelerated digitalization, leading to an exponential increase in the generation and flow of data. This transformation suggests that the privacy landscape is likely to evolve into one that leverages data to maximize organizations' business output, while ensuring adequate protection against risks faced by consumers.

Furthermore, Singapore is home to the regional headquarters of 80% of the world's top 100 tech firms. One of the key factors behind this is Singapore's strong data security framework. Accordingly, strengthening this framework of data protection will remain critical to ensure that Singapore continues to be attractive to foreign investment.

 SOUTH AFRICA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in South Africa.

A dedicated data protection law, the Protection of Personal Information Act 2013 ('POPIA'), became enforceable on 1 July 2021.

1.2 What are the primary laws regulating privacy in South Africa? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

POPIA is the principal Act regulating privacy in South Africa.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation is integrated into POPIA in various ways. The information protection principle of Accountability (see question 4.1) tasks responsible parties with ensuring that they process personal information lawfully and in compliance with POPIA.

Further, POPIA provides for self-regulation through the development of codes of conduct by industry bodies. The Direct Marketing Association of South Africa has developed such a code of conduct, which, although it has yet to receive formal approval by the Information Regulator, provides a useful framework for marketers in respect of best practices when marketing under POPIA.

1.4 How is privacy law enforced in South Africa? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

POPIA established the office of the Information Regulator, which is responsible for overseeing the protection of personal information and enforcing POPIA.

Self-regulatory bodies may apply for the issuing of a code of conduct by the Information Regulator, and once approved, the body must monitor compliance with the code of conduct by its members and handle complaints.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in South Africa?

POPIA applies to the processing of information by or for a responsible party (including a company) domiciled or established in South Africa or processing personal information in South Africa.

2.2 Does privacy law in South Africa apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

POPIA applies to a responsible party domiciled outside the country only if the processing uses automated or non-automated means situated in South Africa. It will not apply where those means (ie, equipment, such as servers, etc) are used only for forwarding personal information. Where information is processed by non-automated means, it must form part of a filing system or be intended to form part of it in order for POPIA to apply.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in South Africa?

‘Personal information’ is defined in POPIA as ‘information relating to an identifiable, living, natural person and where it is applicable, an identifiable existing juristic person’.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

POPIA provides for a category of ‘special personal information’. ‘Special personal information’ is information relating to a data subject’s:

- (a) religious or philosophical beliefs;
- (b) race or ethnic origin;
- (c) trade union membership;
- (d) political persuasion;
- (e) health;
- (f) sex life;
- (g) biometric information; or
- (h) criminal behavior, to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Special personal information is afforded a higher degree of protection and the processing of this information is prohibited unless specific circumstances listed in POPIA are present.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

- (a) **Anonymized data** is not considered to be personal information as it is, by definition, permanently de-identified data, in which the data subject cannot be re-identified. Anonymized data is not subject to POPIA.
- (b) **Pseudonymized data** is treated as personal information under POPIA, because re-identification is still possible where identifiers are replaced with codes or numbers (or any other pseudonyms). One of the obligations of the responsible party under POPIA will be to ensure secure storage of the key or information that can re-identify the data subject.
- (c) **De-identified data** is exempt from POPIA if the data cannot be re-identified. If re-identification is possible, then all relevant requirements for processing personal information will still apply to the data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must ensure compliance with POPIA’s eight information processing principles:

- (a) **Accountability**—An obligation is placed on the responsible party to ensure that the principles for information processing, and all measures giving effect to such principles, are complied with through the entire processing.

- (b) **Processing limitation**—The processing of personal information must be lawful, and information may only be processed if it is adequate, relevant and not excessive given the purpose for which it is processed.
- (c) **Purpose specification**—The collection of personal information must be for a specific and lawful purpose related to a function or activity of the responsible party and the necessary steps must be taken by the responsible party to ensure that the data subject is aware of the purpose which the personal information is being collected, subject to the exemptions in POPIA.
- (d) **Further processing limitation**—An obligation is placed on a responsible party to ensure the further processing of information is compatible with the purpose for which it was initially collected, using the determination criteria included in POPIA.
- (e) **Information quality**—The responsible party must take the necessary steps to ensure that the personal information is complete, accurate, not misleading and updated to the extent necessary, having regard to the purpose for which the personal information is collected or further processed.
- (f) **Openness**—The responsible party must provide the data subject with certain prescribed information, such as:
 - (i) the name and address of the responsible party,
 - (ii) the information being collected, and
 - (iii) whether the supply of the information by the responsible party is voluntary or mandatory.
- (g) **Security safeguards**—The responsible party must take appropriate, reasonable and organizational steps to protect the integrity and confidentiality of the personal information in its possession. In addition, specific obligations are placed on an operator when processing information on behalf of a responsible party.
- (h) **Data subject participation**—A data subject has the right to:
 - (i) access information held by a responsible party or which has been made available to a third party,
 - (ii) request a responsible party to delete inaccurate, irrelevant and unlawfully obtained information, and
 - (iii) request that a responsible party delete information which the responsible party is no longer authorized to retain.

Other key obligations are that companies must appoint an information officer who will be responsible for compliance and must comply with POPIA's rules regarding transferring personal information outside of South Africa.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

POPIA distinguishes between responsible parties and operators:

- (a) A **responsible party** is 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'.
- (b) An **operator** is 'a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party'.

A responsible party will be obliged to conclude an operator agreement with an operator in order to regulate the operator's processing of personal information for the responsible party.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, a responsible party may only process personal information if one or more of the following legal lawful bases apply:

- (a) consent;
- (b) contractual necessity;
- (c) legal obligation;
- (d) legitimate interest of the data subject;
- (e) public law duty; or
- (f) legitimate interest of the responsible party or a third party to whom the information is supplied.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

A privacy notice should clearly and accurately inform data subjects about how their personal information is being collected, used, and protected. It should include:

- (a) the responsible party's contact details;
- (b) the types of information collected;
- (c) the purposes of processing the personal information (specifying the types of advertising to be conducted);
- (d) the category or description of recipients of the personal information;
- (e) whether providing personal information is voluntary;
- (f) what the implications are if the data subject does not provide it (eg, less relevant advertisements);
- (g) the data subject's rights; and
- (h) contact details for the Information Regulator.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

POPIA affords data subjects various rights in relation to the processing of their personal data. These rights include the right to request the correction, destruction or deletion of the subject's personal information. The data subject can request that personal data be deleted if the data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or if the responsible party no longer has the authority to be in possession or control of the personal information.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

- (a) To be valid under POPIA, consent must be:
 - (i) **voluntary**—not forced or a condition for using a service;
 - (ii) **specific**—for a clearly defined purpose;

- (iii) **informed**—the data subject must be provided with enough information to make an informed decision, including the nature of the information, the purpose of processing, and the rights they have; and
 - (iv) **documented**—the responsible party must be able to show that the data subject provided consent.
- (b) Consent is mandatory if:
 - (i) the data subject has not previously interacted with the company (ie, there is no existing customer relationship); and
 - (ii) the company wants to send direct marketing via email, SMS, fax, or automated calls.
- (b) However, POPIA provides for a ‘soft opt-in’ in terms of which companies may market without prior consent if:
 - (i) the data subject is an existing customer of the company;
 - (ii) the marketing is for the company’s own similar products or services; and
 - (iii) the data subject has been given a reasonable opportunity to opt out, both at the time of collection of the personal information and in every subsequent marketing communication.
- (d) It is necessary to provide an opt-out option in every advertising message, which must offer:
 - (i) clear and simple opt-out methods (eg, an unsubscribe link, SMS stop command, cookie settings);
 - (ii) real-time or prompt response to opt-out requests; and
 - (iii) no cost or penalty for opting out.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Responsible parties that engage vendors or third parties in advertising—such as advertising agencies, demand-side platforms (‘DSP’s), supply-side platforms (‘SSP’s), data brokers, or analytics providers—must ensure that any sharing or processing of personal information by these parties complies with POPIA’s requirements.

Most advertising vendors (eg, DSPs and advertising agencies) will be operators, but some (such as data brokers or analytics platforms) may act as independent responsible parties depending on how they use the personal information.

POPIA requires:

- (a) that a data protection agreement is signed between the responsible party and any advertising vendors, which must require that the operator establishes and maintains the necessary security measures;
- (b) that the responsible party conducts due diligence on the advertising vendor’s data practices;
- (c) transparency regarding third parties that receive personal information;
- (d) a lawful basis (usually consent) for sharing personal information for advertising purposes; and
- (e) that personal information that is shared with advertising vendors must only be used for the specified advertising purpose.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

- (a) The contractual requirements and best practices to adhere to when engaging with vendors are as follows:
 - (i) implement appropriate technical and organizational security measures;
 - (ii) prevent loss, damage, unauthorized destruction, and unlawful access to personal information;
 - (iii) only process personal information with the knowledge or authorization of the responsible party;
 - (iv) don't use personal information for any other purpose;
 - (v) sub-processing prohibited without prior written approval, and sub-processors required to be bound by equivalent contractual obligations;
 - (vi) if personal information is transferred to a vendor outside of South Africa, the contract must ensure the vendor provides an adequate level of protection and include standard contractual clauses or binding obligations to safeguard the data.;
 - (vii) return or destroy personal data upon request or termination of the agreement;
 - (viii) provide written confirmation of data deletion if requested; and
 - (ix) include rights to conduct audits or assessments and receive information on the operator's compliance efforts.
- (b) The obligations that companies must fulfil when receiving personal information are as follows:
 - (i) confirm that the third party had a lawful basis for collecting and sharing personal information (eg, consent);
 - (ii) ensure that the data subject was informed that their personal information may be shared with the company; and
 - (iii) include warranties and indemnities in the contract regarding the lawful collection and sharing of personal information.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

- (a) **Internal Due Diligence (Self-Assessment)**
 - (i) Personal Information Impact Assessment:
 - evaluate how personal information is collected, used, shared, and stored;
 - identify risks to data subjects and the business;
 - required when introducing new technologies or new processing activities (eg, behavioral profiling, biometric processing).
 - (ii) Records of processing activities: Keep detailed records of:
 - what data is collected;
 - the purpose of processing;
 - the legal basis for processing personal information;
 - retention periods;
 - recipients (including third parties).

- (iii) Legal basis assessment:
 - ensure each processing activity has a valid lawful basis (eg, consent, legitimate interest, contractual performance);
 - document the justification.
- (iv) Information security assessment:
 - conduct regular audits of IT systems and access controls;
 - ensure that technical and organizational safeguards comply with POPIA.
- (b) **Third-party due diligence (vendor risk management)**
 When working with third parties (eg, processors, advertising platforms, cloud services):
 - (i) Assess the vendor's:
 - data security practices (eg, encryption, access controls);
 - compliance certifications (eg, ISO 27001, SOC 2); and
 - privacy policies and practices.
 - (ii) Contractual safeguards:
 - ensure a data processing agreement is in place.
 - (iii) Cross-border transfer protections:
 - check whether data will be transferred outside South Africa; and
 - ensure appropriate safeguards or adequacy mechanisms are in place.
- (c) **Due diligence for high-risk activities:**
 Additional scrutiny is required for:
 - (i) processing children's data;
 - (ii) automated decision-making or profiling;
 - (iii) biometric or special personal information; and
 - (iv) use of AI, data analytics, or tracking technologies.
 For these, companies should:
 - conduct risk assessments;
 - implement additional privacy controls;
 - seek legal advice where necessary.
- (d) **Ongoing monitoring and review:**
 Due diligence is not a one-off activity. Companies must:
 - (i) Periodically review their processing activities and vendor relationships;
 - (ii) Update contracts and policies to reflect regulatory changes;
 - (iii) Audit high-risk vendors regularly.
- (e) **Document everything:** POPIA requires companies to be accountable. This means:
 - (i) Keeping evidence of consent.
 - (ii) Documenting decisions on lawful basis.
 - (iii) Keeping records of risk assessments.
 - (iv) Demonstrating vendor vetting and monitoring.

Impact assessments ('Personal Information Impact Assessments') are required when a company undertakes processing that poses a reasonably foreseeable risk to the rights and freedoms of data subjects. In the context of advertising, this includes any use of personal information that may be intrusive, involve sensitive data, or the use of novel or high-risk technologies.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

POPIA regulates direct marketing on a soft opt-in or opt-in basis (see question 5.3).

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies, such as cookies, are not specifically regulated in South Africa; however, the principles of POPIA apply, even though this aspect is not directly addressed by POPIA.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs process a lot of information and thus are also governed by all the principles of POPIA in respect of the processing of customers' personal information. This may include, amongst other things, obtaining the consent from the customer to track their purchases in order to promote products in the future based on the customer's buying patterns or notifying the customer that their information will be used for this purpose.

7.4 How is social media and influencer marketing regulated under privacy law?

In the same fashion as other customer information: any and all information collected or shared via social media is governed by POPIA.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

This is not specifically regulated in South Africa; however, the principles of POPIA apply, even though this aspect is not directly addressed by POPIA.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

These are regulated by POPIA as follows:

(a) Digital identity resolution

- (i) Processing limitation: Any linking of data to identify a person is 'processing' and must have a lawful basis (consent, contractual necessity, legitimate interest, etc);
- (ii) Purpose specification: Data collected for one purpose cannot be used for another (such as identity linking) unless it is compatible or fresh consent is obtained;
- (iii) Transparency and openness:
 - Responsible parties must inform data subjects that their information may be used for profiling or identity resolution.
 - Privacy notices must disclose the use of tracking and matching technologies.
- (iv) Data minimization: Only the minimum data necessary should be collected and linked.
- (v) Automated decision-making: If identity resolution feeds into profiling or decisions with legal effects (eg, credit scoring, advertisement targeting), the data subject has the right to request human intervention.

- (b) **Data clean room technologies**
 - (i) NB de-identification does not equal exemption:
 - If data is only pseudonymized (ie, re-identification is possible), POPIA still applies.
 - True anonymization (irreversible de-identification) may exempt the data from POPIA, but must be legitimately irreversible.
 - (ii) Cross-party processing:
 - Joint controllers or independent parties using clean rooms must have written agreements detailing responsibilities and ensuring compliance with POPIA.
 - They must uphold accountability and security safeguards (eg, data use restrictions, audit trails).
 - (iii) Security safeguards:
 - Clean rooms must have technical and organizational measures to prevent unauthorized re-identification or misuse.
 - Use of data access controls, encryption, and secure logging is essential.
 - (iv) Transparency: Data subjects should be made aware (via privacy notices) that their data may be used in aggregated or de-identified formats for analytics or advertising.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is regulated under POPIA because it involves the collection and use of geolocation data, which qualifies as personal information. Note in particular:

- (a) **Lawful basis for processing location data:** Processing must be based on one of the lawful grounds under POPIA, usually:
 - (i) informed and voluntary consent (most common for LBA);
 - (ii) contractual necessity (less common unless location is core to the service); or
 - (iii) legitimate interest, provided it does not override privacy rights (used cautiously).
- (b) **Transparency and notice:** You must clearly inform the data subject of:
 - (i) what location data is being collected;
 - (ii) how and why it is used for advertising;
 - (iii) with whom it may be shared; and
 - (iv) their rights (eg, to object or withdraw consent).
- (c) **Data minimization and purpose limitation:**
 - (i) collect only the data needed for the specific advertising purpose;
 - (ii) do not use the data for unrelated purposes without renewed consent; and
 - (iii) avoid collecting continuous or background location data unless necessary and explicitly consented to.
- (d) **Security safeguards:**
 - (i) protect geolocation data using encryption, access controls, and pseudonymization where possible; and
 - (ii) regularly assess risks of re-identification or tracking misuse.
- (e) **Right to object and opt-out:**
 - (i) data subjects have the right to object to their personal information being used for direct marketing or profiling, including via location data;
 - (ii) provide easy-to-use opt-out mechanisms, such as toggles in apps or 'unsubscribe' links.

7.8 How are data brokers defined and regulated under privacy law?

POPIA does not contain provisions relating directly to data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

Although children's personal information is not classified as special personal information or a separate category of personal information, POPIA contains specific provisions relating to the processing of children's personal information.

Processing a child's personal information is prohibited unless:

- (a) a competent person (eg, parent or guardian) consents; or
- (b) the processing is necessary for:
 - establishing or defending a legal right or obligation,
 - compliance with a legal obligation, or
 - historical, statistical, or research purposes (with security safeguards);
- (c) done by a public body as part of its lawful functions; or
- (d) approved by the Information Regulator.

Therefore, advertising or marketing to children requires prior parental or guardian consent.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

- (a) **Profiling:** POPIA does not explicitly mention profiling, however as profiling relies on various types of personal information, including demographic information, behavioral data as well as people's values, beliefs, and lifestyles, POPIA is applicable thereto.
- (b) **Automated decision-making:** A data subject may not be subject to a decision based solely on automated processing if that decision results in legal consequences or affects them to a substantial degree, unless the decision is:
 - (i) taken in connection with entering into or performing a contract: and
 - the request of the data subject in terms of the contract has been met; or
 - appropriate measures have been taken to protect the data subject's legitimate interests, or
 - (ii) governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.
- (c) **Requirements for profiling or automated decision making in advertising**
 - (i) Always obtain informed consent, especially for behavioral or sensitive targeting, and provide simple and effective opt-out mechanisms such as 'unsubscribe' links, privacy settings and cookie controls;
 - (ii) Disclose profiling clearly in privacy notices and interfaces (transparency);
 - (iii) Allow data subjects to request human review of significant automated decisions;
 - (iv) Avoid profiling minors unless legally justified and parental/guardian consent is obtained;
 - (v) Conduct privacy impact assessments when using AI for profiling;
 - (vi) Implement bias detection and algorithmic fairness checks; and
 - (vii) Ensure that contracts with technology partners include data protection clauses.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

POPIA prohibits the transferring of data to third parties in a foreign country unless one or more of the following circumstances are apparent:

- (a) the recipient of such data is subject to a law, a binding code of conduct or a contract which upholds the principles for reasonable processing of information in a similar fashion to the information principles set out in POPIA;
- (b) the data subject consents to the transfer;
- (c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- (d) the transfer is necessary for the conclusion of a contract in the interest of the data subject between the responsible party and third party; or
- (e) the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to the transfer and, if such consent could be obtained, the data subject would most likely give the necessary consent.

Examples of safeguards required in order to transfer data to third parties in a foreign country are the following:

- data protection agreements with third-party processors;
- due diligence reports on the recipient country's data protection environment; or
- technical measures such as encryption and access controls.

POPIA does not mandate standard contractual clauses; however, mechanisms such as contractual clauses or agreements ensuring adequate data protection safeguards and internal policies and procedures (such as binding corporate rules for multinational companies) are required.

POPIA does not prohibit transfers to specific countries or jurisdictions, however if the recipient cannot guarantee an adequate level of protection, and no exception applies, the transfer will be unlawful.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Data protection is still a very new area of the law in South Africa. Accordingly, issues will arise in the course of the development of this law.

Considering that POPIA provides for specific circumstances in which data may be transferred to a third party based in a foreign country, a subsidiary in South Africa would need to abide by these provisions when transferring to the holding company in another country, even though the data is being transferred between group companies.

POPIA provides for the adoption of binding corporate rules ('BCR's) by multinational companies which set data protection standards that the group is required to adhere to, which BCRs would allow for the transfer of personal information between entities within the group under POPIA.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in South Africa? Are there minimum standards? Does this differ by sector or size of the entity?

POPIA requires a responsible party to secure the integrity of personal information in its possession by taking appropriate, reasonable, technical and organizational measures to prevent any loss or unauthorized destruction of, unlawful access to, or processing of personal information. In addition, a responsible party must take reasonable measures to:

- (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- (b) establish and maintain appropriate safeguards against the risks identified;
- (c) regularly verify that the safeguards are efficiently implemented; and
- (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Lastly, a responsible party and operator must have regard to generally accepted information security practices and procedures which apply to it or may apply to it in respect of a specific industry or professional rules and regulations. No specific standards have been prescribed as yet.

9.2 How are personal data breaches regulated in South Africa? What are the requirements for notification and response?

A security compromise occurs when personal information has been accessed or acquired by any unauthorized person. POPIA requires that the responsible party must notify the Information Regulator and the data subject when a security compromise has taken place.

The data subject must be notified in writing as soon as reasonably possible once it has been discovered that there has been a security breach, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the breach and to restore the integrity of the responsible party's information system. A delay in notification of the data subject may only occur if the South African Police Services, the National Intelligence Agency or the Information Regulator directs that notification will impede a criminal investigation.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

A person convicted of an offence in terms of POPIA can be sanctioned with a fine and/or imprisonment. In cases where the offender has hindered, obstructed or unlawfully influenced the Information Regulator, the term of imprisonment may be up to 10 years. In any other case, the imprisonment period may not exceed 12 months. POPIA also provides for the imposition of an administrative fine, which may not exceed ZAR10 million (approx USD 550,000).

10.2 Do consumers have a private right of action? What remedies are available to them?

A data subject or, at the request of the data subject, the Information Regulator may initiate a civil action for damages in a court against the responsible party for interference with the protection of personal

information, irrespective of intent or negligence on the part of the responsible party. A court hearing such proceedings may award an amount which is deemed just and equitable, which may include payment of damages, aggravated damages, interest and the costs of the lawsuit.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Since POPIA became fully effective on 1 July 2021, the Information Regulator has increasingly asserted its authority, although its approach has leaned more toward education and compliance support than aggressive enforcement.

Examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising:

- (a) **FT Rams Consulting Direct Marketing Complaint:** FT Rams Consulting was accused of sending unsolicited direct marketing emails despite the data subject opting out multiple times and requesting removal from the company's mailing list.
The first ever enforcement notice under POPIA for a direct marketing complaint was issued, in the terms of which FT Rams Consulting was ordered to:
 - (i) immediately cease all unsolicited marketing via electronic communications unless prior consent is obtained;
 - (ii) ensure that the first contact with a new data subject is solely for the purpose of requesting consent, and to do so only once;
 - (iii) use the Regulator's prescribed consent form;
 - (iv) develop and maintain a database of data subjects who have not consented or have previously opted out; and
 - (v) submit proof of compliance within 90 days of receipt of the notice. Failure to comply would result in a fine of up of ZAR 10 million and/or imprisonment of up to 10 years.
- (b) **MiWay Insurance—King Goodwill Zwelithini:** MiWay Insurance allegedly processed the personal information of King Goodwill Zwelithini without his consent. Concerns were raised that his personal information may have been used for direct marketing purposes, which would violate the conditions for lawful processing under POPIA.
The Regulator noted the media reports and issued a public statement outlining the relevant provisions of POPIA, including: the need for consent or another lawful basis for processing personal information; the requirement to collect personal information directly from the data subject; the obligation to ensure the security and confidentiality of personal information; and the right of a data subject to object to direct marketing.
At the time, some sections of POPIA were not yet in force, so a formal complaint could not be lodged under the full powers of POPIA. However, despite the legal limitations, the Regulator announced its intention to proactively engage MiWay to assess:
 - (i) What processes and measures the company had implemented for POPIA compliance;
 - (ii) Whether the processing of the King's personal information met the standard of lawful processing.
- (c) **Guidance Note on the Processing of Personal Information of Voters, and the Countering of Misinformation and Disinformation During Elections:** While not an enforcement action or lawsuit, the guidance note provides some key insights into expectations for the enforcement of POPIA. The guidance note provides directions to political parties and candidates on the lawful use of personal information for campaigning and donation requests.

Key Points:

- (i) Political persuasion is a special category of personal information; its use is restricted;
- (ii) Consent is required for unsolicited electronic communication (eg, SMS, email, auto-calls) for donations; and
- (iii) Campaign data must be:
 - collected lawfully, with transparency,
 - limited to the minimum required, and
 - not used for secondary purposes without consent.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in South Africa?

There are currently no rules particular to the culture of South Africa which affect privacy.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Enforcement of POPIA in South Africa is particularly focused on:

- (a) security safeguards;
- (b) direct marketing without consent;
- (c) children's personal information;
- (d) failure to notify data breaches; and
- (e) cross-border transfers without adequate protection.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

In most jurisdictions, 'personal information' is limited to the personal information of natural persons (humans). However, POPIA's definition extends to the personal information of legal persons (including companies). This means that responsible parties must comply with POPIA's requirements when they process personal information of both natural persons and legal persons.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, South Africa's data privacy landscape has evolved significantly, with key developments enhancing the enforcement and scope of POPIA. Below is an overview of the most notable changes:

- (a) **Introduction of the eServices Portal for Data Breach Reporting (April 2025):** On April 7, 2025, the Information Regulator mandated that all data breaches, termed 'security compromises,' be reported through a new online e-Services Portal. This move streamlines the reporting process and aligns South Africa with global best practices in breach notification.
- (b) **First Enforcement Notice for Direct Marketing Non-Compliance (February 2024):** The Information Regulator issued its inaugural enforcement notice against a company for failing to comply with POPIA's direct marketing provisions. This action underscores the Regulator's commitment to enforcing compliance in marketing practices.

- (c) **Significant Fine Imposed on Department of Justice (July 2023):** In a landmark decision, the Department of Justice and Constitutional Development was fined ZAR 5 million (approx USD 277,000) for inadequate cybersecurity measures, marking the first substantial penalty under POPIA. The Department had failed to renew critical cybersecurity licenses, compromising personal information protection.
- (d) **Amendments to POPIA Regulations (April 2025):** The Information Regulator introduced amendments to POPIA regulations, simplifying processes for data subjects to object to data processing, request corrections or deletions, and manage consent for direct marketing. Additionally, these amendments introduced new responsibilities for information officers and allowed for administrative fines to be paid in installments.
- (e) **Constitutional Court Ruling on Access to Tax Records (May 2023):** In the case of *Arena Holdings v South African Revenue Service*, the Constitutional Court ruled that certain provisions restricting access to tax records were unconstitutional. This decision emphasizes the balance between privacy rights and the public's right to information.
- (f) **Publication of Direct Marketing Guidance Note (December 2024):** The Information Regulator released a guidance note clarifying the requirements for direct marketing under POPIA. Key points include the necessity of obtaining informed, voluntary, and specific consent before engaging in direct marketing activities, and the limitation of one unsolicited communication to request such consent.
- (g) **Information Regulator's Focus on AI and Data Privacy (April 2025):** Recognizing the growing impact of artificial intelligence, the Information Regulator announced initiatives to ensure AI technologies are used ethically and that personal information remains protected in the evolving digital landscape.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Data protection law imposes onerous obligations on companies. This burden is increased due to the complexities created by information technology and the large quantity of data processed by companies. This requires companies to invest in technology infrastructure and human resources and service providers. This may be particularly burdensome for small businesses, especially since organizations will need to monitor, upgrade and invest in their technology on a constant basis in order to ensure that they remain compliant.

12.3 What do you envision the privacy landscape will look like in five years?

Organizations will be more focused on privacy compliance, in order to adhere to POPIA's requirements, and also due to continuous developments and improvements in information technology.

Data subjects will also be more aware of their rights and will probably be quite active in enforcing them.

 SOUTH KOREA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in South Korea.

In Korea, there are various laws, regulations and guidelines that govern privacy as discussed at question 1.2.

Government agencies function as regulators (see questions 1.3 and 1.4).

1.2 What are the primary laws regulating privacy in South Korea? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary laws regulating privacy in Korea are:

- (a) **Personal Information Protection Act ('PIPA')**: PIPA serves as the primary legislation governing the processing and safeguarding of personal data. It regulates the entire lifecycle of personal information—including collection, use, provision, retention, and destruction—by defining the rights of data subjects and the obligations of data controllers and processors. It also stipulates sanctions for violations of its provisions;
- (b) **Credit Information Use and Protection Act ('Credit Information Act')**: The Credit Information Act governs the processing of personal credit information by credit information companies, financial institutions, public agencies, and other relevant entities;
- (c) **Act on the Protection and Use of Location Information ('Location Information Act')**: The Location Information Act regulates the processing of location information, particularly focusing on businesses engaged in the collection and use of personal location data;
- (d) **Act on the Promotion of IT Network Use and Information Protection ('Network Act')**: Previously, the Network Act regulated the processing of personal data by telecommunications service providers. However, with the enactment of the amended Network Act on August 5, 2020, most provisions concerning personal data protection were transferred to PIPA. The current Network Act continues to regulate certain aspects of personal data processing, such as restrictions on the transmission of advertising information for commercial purposes; and
- (e) **Medical Service Act**: The Medical Service Act governs the handling of medical-related personal information, such as personal data contained in medical records and electronic prescriptions.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

In the context of advertising practices, requirements regarding privacy and consumer protection are detailed in guidelines issued by the PIPC or the KCC. Self-regulation primarily involves compliance with these guidelines.

In addition, data controllers can voluntarily establish privacy protection frameworks by obtaining certification under the Information Security Management System or the Information Security and Privacy Management System, both of which are operated by the Korea Internet & Security Agency ('KISA').

1.4 How is privacy law enforced in South Korea? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The enforcement of privacy regulations in Korea is primarily overseen by the Personal Information Protection Commission ('PIPC'). The PIPC is responsible for establishing policies, systems, and plans related to personal data protection, investigating personal data breaches, ordering corrective actions or imposing administrative fines, and mediating personal data-related disputes. In addition, the PIPC develops and distributes various guidelines to help data controllers clearly understand and comply with their legal obligations. These guidelines provide detailed examples and procedures to assist with the practical application of the provisions of the PIPA. Data controllers in Korea are expected to implement privacy protection measures in accordance with these guidelines.

Separately, the Financial Services Commission ('FSC') and the Financial Supervisory Service ('FSS') regulate the processing of personal credit information under the Credit Information Act.

The Korea Communications Commission ('KCC') regulates the processing of personal location information under the Location Information Act and supervises the processing of information in the course of providing information and communications services under the Network Act.

In cases where a data subject suffers damages due to a violation of privacy laws, the data subject may bring a civil claim for damages. The PIPA provides punitive damages and statutory damages systems to ensure the effectiveness of such claims.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in South Korea?

Under the PIPA, the term 'data controller' is defined as public institutions, corporations, organizations, and individuals who process personal data either on their own or through others in order to manage personal data files for business purposes. Accordingly, companies that process personal data for business purposes are considered data controllers and are therefore subject to the requirements of the PIPA.

2.2 Does privacy law in South Korea apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The PIPA does not explicitly address whether it applies to foreign companies. However:

- (a) The PIPC interprets that the PIPA may apply where a foreign business operator:
 - (i) provides goods or services globally,
 - (ii) processes personal information of Korean data subjects or Korean nationals overseas, or
 - (iii) processes personal information within the territory of Korea.
- (b) In practice, the PIPC determines the applicability of the PIPA on a case-by-case basis, considering:
 - (i) whether the foreign business operator provides goods or services to Korean data subjects,
 - (ii) the extent to which the operator's data processing activities impact Korean nationals and Korean data subjects, and
 - (iii) whether the operator maintains a place of business in Korea.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in South Korea?

According to the PIPA, ‘personal information’ refers to information about a living individual that falls under any of the following categories:

- (a) information that can identify an individual, such as name, resident registration number, and images;
- (b) information that, although not capable of identifying an individual on its own, can easily be combined with other information to identify the individual. In this case, the ease of combination should be reasonably considered based on factors such as the availability of other information, the time, cost, and technology required to identify the individual; and
- (c) information that, by pseudonymization, cannot identify a specific individual without the use or combination of additional information to restore it to its original state (‘pseudonymized information’). ‘Pseudonymization’ refers to processing personal information in a manner that, by deleting or replacing part or all of the information, ensures that the individual cannot be identified without the use of additional information.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

According to the PIPA and its Enforcement Decree, ‘sensitive information’ refers to information concerning a person’s thoughts, beliefs, membership or withdrawal from labor unions or political parties, political views, health, sexual life, or genetic information, information corresponding to criminal records, biometric information generated for the purpose of identifying a specific individual, and information about race or ethnicity.

For such sensitive information as above, a data controller shall not process sensitive information, except for the following circumstances:

- (a) if the data controller obtains a separate consent from the data subject for the processing of sensitive information, distinct from the consent for the processing of other personal information; or
- (b) if the processing of sensitive information is required or permitted by law.

Additionally, if sensitive information may be disclosed during the provision of goods or services, the data controller must inform the data subject of the possibility of such disclosure in advance, include this information in the privacy policy, and provide the data subject with an option to withhold disclosure.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

- (a) **Anonymized information:** Anonymized information refers to data that, even when combined with other information, cannot be used to identify a specific individual, taking into account factors such as time, cost, and technological capability. Since anonymized information does not constitute personal information under the PIPA, data controllers are free to process it without any restrictions on its intended use.

- (b) **Pseudonymized information:** Pseudonymized information is defined as information that, through pseudonymization, cannot identify a specific individual without the use or combination of additional information. Although pseudonymized information alone does not identify a specific individual, there remains a possibility that an individual could be identified when it is combined with other information.

Under the PIPA, data controllers may process pseudonymized information without obtaining the data subject's consent for purposes such as statistical compilation, scientific research, or the preservation of public records. When processing pseudonymized information, data controllers must take necessary technical, managerial, and physical measures to ensure the security of the information and to prevent its loss, theft, leakage, forgery, alteration, or destruction. This includes separately storing and managing any additional information that could be used to re-identify individuals. To manage the processing of pseudonymized information, data controllers must maintain processing records and retain them for at least three years after the destruction of the pseudonymized information.

The combination of pseudonymized information between different data controllers must be carried out by a specialized agency designated by the PIPC or the head of the relevant central administrative agency. In order to export the combined information outside the specialized agency, a data controller must pseudonymize or anonymize the data and obtain approval from the head of the specialized agency.

Data controllers processing pseudonymized information must not use it for the purpose of identifying specific individuals. If, during the course of processing, data that could identify a specific individual is generated, the data controller must immediately cease processing and promptly retrieve and destroy such data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Under the PIPA, companies that collect or process personal information have several core obligations. These are broadly aligned with global privacy frameworks such as the GDPR, but have distinct features tailored to the Korean regulatory context:

- (a) **Transparency/notice obligations:** data controllers are required to draft and publish a privacy policy on their company websites, which must include the following details:
- (i) purpose of personal information processing;
 - (ii) duration of processing and retention;
 - (iii) matters related to third-party provision of personal information (if applicable);
 - (iv) procedures and methods for personal information destruction;
 - (v) potential disclosure of sensitive information and available opt-out options (if applicable);
 - (vi) matters related to outsourcing of personal information processing to third parties (if applicable);
 - (vii) matters concerning the processing of pseudonymized information (if applicable);
 - (viii) rights and obligations of data subjects and their legal representatives, including methods for exercising these rights;

- (ix) name of the chief privacy officer or contact details of the relevant department/team responsible for overseeing personal information protection and addressing data subjects' grievances;
 - (x) matters concerning the installation and operation of devices that automatically collect personal information, such as internet access data files, and procedures for opting out of such collection (if applicable);
 - (xi) types of personal information being processed; and
 - (xii) measures taken to ensure the security of personal information.
- (b) **Data subject rights:** data subjects have the right to do the following, and the data controller must respond within 10 days and can only refuse with legitimate reasons:
- (i) request access to their personal information;
 - (ii) request the correction, suspension, or deletion of their personal information;
 - (iii) withdraw consent for the collection and use of their personal information; and
 - (iv) refuse automated decision-making or request explanations regarding such decisions.
- (c) **Data minimization and purpose limitation:** data controllers must clearly define the purpose of personal information processing and collect only the minimum amount of personal information necessary to achieve that purpose. Processing should be conducted appropriately and within the scope necessary for the original purpose; it must not extend beyond that purpose. Also, when personal information becomes unnecessary, the data controller must destroy it without delay.
- (d) **Record-keeping:** data controllers are also required to retain and manage records such as access logs to personal information processing systems and records of changes to access rights to such systems for a prescribed period.
- (e) **Employee training:** data controllers must regularly provide necessary training to the chief privacy officer and any personnel handling personal information.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

A data controller processes personal information under its own responsibility and bears the associated legal obligations. A data controller may entrust the processing of personal information to a third party ('trustee') by entering into a data processing agreement. If the trustee violates the PIPA while processing personal information in connection with the entrusted tasks, the data controller remains liable for such violations.

An trustee entrusted with the processing of personal information may only process the data within the scope of the entrusted tasks and, within that scope, assumes the obligations and responsibilities of a data controller.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Under the PIPA, data controllers must have a lawful basis for collecting and using personal data. They may process personal data under the following circumstances:

- (a) where they obtain explicit prior consent from the data subject;
- (b) where specific provisions in law authorize the processing;

- (c) where the processing is necessary to take action at the request of the data subject during the process of entering into or performing a contract with them; or
- (d) where achieving the legitimate interests of the data controller clearly outweighs the rights of the data subject.

Previously, data controllers primarily relied on the data subject's consent as the lawful basis for processing personal data. However, the 2023 amendment to the PIPA permits data controllers to process personal data without obtaining consent when it is necessary for entering into or performing a contract with the data subject. In practice, despite this amendment, it remains common for data controllers to rely on the data subject's consent for the processing of personal data.

Meanwhile, when processing sensitive information or unique identification information, or when providing personal data to third parties, data controllers must obtain separate and explicit consent from the data subject.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

When processing personal data for advertising purposes, companies must clearly state in their privacy policy that personal data will be processed for advertising purposes and specify the lawful basis for such processing (typically, the data subject's consent). If personal data processing for advertising purposes is outsourced to a third party, the privacy policy must also include information regarding the entrustment of such processing.

Additionally, since data subjects have the right to withdraw their consent to the processing of their personal data, the privacy policy must describe the procedures through which data subjects can exercise their right to withdraw consent.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

When transmitting promotional information, companies must obtain explicit prior consent from data subjects through either written or verbal means.

Consumers have the following rights with respect to their personal data:

- (a) the right to request access to their personal information;
- (b) the right to request the correction, suspension, or deletion of their personal information;
- (c) the right to withdraw consent for the collection and use of their personal information; and
- (d) the right to refuse automated decision-making or to request an explanation regarding such decisions.

Consumers may withdraw their consent to receive promotional information at any time, and the sender must immediately honor such withdrawal. Consumers shall not bear any monetary costs, such as telephone charges, incurred when withdrawing consent or refusing to receive promotional information.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Since the processing of personal data for advertising purposes is not essential for the provision of services, companies must obtain separate consent from data subjects before engaging in such processing.

However, exceptions apply in the following cases:

- (a) if a person who collected the recipient's contact information directly through a transaction involving goods, etc, intends to send promotional information for commercial purposes regarding goods of the same type as those traded with the recipient, within a specific period of time; or
- (b) if a telemarketing seller informs the recipient of the source of their personal information orally and then proceeds with the telemarketing call.

Because data subjects have the right to withdraw their consent to the processing of personal data for advertising purposes, companies must provide opt-out options for advertising activities. When sending promotional information, companies must also clearly inform recipients of the methods available to express their intention to withdraw consent.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The transfer of personal information to a third party is categorized into two types under the PIPA:

- (a) **Third-party provision**, where personal information is transferred for the business operations and interests of the recipient; and
- (b) **Processing entrustment**, where personal information is transferred for the business operations and interests of the entrusting party in relation to the work outsourced to the entrusted party.

The use of vendors in advertising typically constitutes processing entrustment. In this case, the data controller is not required to obtain separate consent from data subjects for the entrustment of processing. However, the data controller must:

- (1) enter into a data processing agreement with the entrusted party (the trustee);
- (2) disclose the purpose of the outsourcing and the name of the trustee in the privacy policy; and
- (3) appropriately supervise the trustee's handling of the personal data.

On the other hand, if the transfer constitutes a third-party provision, the data controller must obtain separate, explicit consent from the data subject for the third-party provision.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Data controllers must process personal data within the scope of the purposes consented to by the data subject or as permitted by law. If a data controller intends to disclose or receive personal data to or from vendors or other third parties beyond the original purpose for which consent was obtained, the data controller must obtain separate, explicit consent from the data subject.

When a data controller entrusts personal data processing to a third party, a written agreement must be executed. The agreement must specify:

- (a) the purpose and scope of the entrusted tasks;
- (b) the technical and managerial measures to protect personal data; and
- (c) the procedures for monitoring and supervising the management of personal data by the entrusted party.

Companies must ensure that the entrusted party complies with these contractual obligations. The entrusted party must not use the personal data beyond the scope of the entrusted purpose.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Under the PIPA, certain public institutions are required to conduct a privacy impact assessment ('PIA') and submit the results to the PIPC. However, for private-sector data controllers, conducting a PIA is not mandatory under the PIPA.

Nevertheless, according to PIPC-issued regulations and guidelines, data controllers are required to establish and implement an internal management plan to ensure the security of personal information. Such internal management plans must include detailed measures, such as the establishment of a privacy protection organization, designation of a chief privacy officer, supervision and training of personnel handling personal information, management and control of access rights, encryption of personal information, retention and inspection of access logs, and the prevention of malicious software.

When a data controller entrusts personal information processing to a third party (trustee), it must enter into an entrustment contract (data processing agreement) that clearly specifies:

- (a) a prohibition on processing personal data for purposes other than those specified in the agreement;
- (b) measures for the technical and managerial protection of personal data;
- (c) a description of the entrusted tasks; and
- (d) limitations on further sub-entrustments.

The data controller must also supervise and manage the trustee to ensure that personal information processing tasks are properly executed and that appropriate security measures are implemented. This evaluation should encompass factors such as the trustee's staffing, physical infrastructure, financial resources, technological capability, and overall accountability.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Network Act specifically regulates the methods for transmitting commercial advertisements. To send commercial advertisements, explicit prior consent must be obtained from the recipient. When sending commercial advertisements through channels other than email (such as SMS, app push notifications, or phone calls), companies may only do so on weekdays between 8:00 am and 9:00 pm. Advertisements must be clearly labelled with '(Advertisement)' and must include the sender's name, contact information, and clear instructions on how to opt out.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

When a data controller installs or operates devices that automatically collect personal information—such as cookies or similar technologies—on websites or applications it operates, it must disclose relevant information in its privacy policy. The privacy policy must include a basic explanation regarding the use of cookies and similar technologies, including the nature of the technology, its purposes, the methods of collecting personal information, and how users can refuse the use of such technologies. The privacy policy must also describe the categories of personal information collected through these technologies.

Additionally, if real-time data (such as log information) can be easily combined with other data to identify an individual, such data will be considered personal information and will be protected under the PIPA. In such cases, the data controller must obtain the data subject's consent before collecting this information.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific privacy regulations under the PIPA that exclusively govern loyalty programs and promotions. Data controllers must instead comply with the general principles applicable to the processing of personal information, including obtaining appropriate consent where necessary and limiting the collection, use, and retention of personal data to what is necessary for the operation of such programs.

7.4 How is social media and influencer marketing regulated under privacy law?

There are no specific privacy regulations under the PIPA that exclusively govern social media and influencer marketing. However, if personal information is collected, used, or otherwise processed in the course of such activities, data controllers must comply with the general principles applicable to the processing of personal information, including obtaining appropriate consent where necessary.

Separately, advertising through social media or influencers in a manner that prevents consumers from recognizing the content as advertising (so-called 'hidden advertising') may violate the Act on Fair Labeling and Advertising and may be subject to enforcement action by the Korea Fair Trade Commission ('KFTC').

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising typically involves the use of behavioral information, which may constitute personal information under the PIPA. For example, where a company collects behavioral information through user identifiers from service subscribers, and such information is combined with separately collected membership information using the user identifier as a key, the behavioral information is considered personal information. Conversely, behavioral information that is processed without identifying a specific individual is not regarded as personal information under the PIPA.

When collecting or using behavioral information that qualifies as personal information, data controllers must, in principle, obtain the data subject's consent.

Where behavioral information does not constitute personal information, consent is not required; however, companies must still comply with the guidelines issued by regulators such as the PIPC.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

While there are no specific laws or regulations governing digital identity, the government has shown support for advancing a digital identification system. The Ministry of the Interior and Safety, in collaboration with the Korean National Police Agency, has introduced the mobile driver's license, which holds the same legal validity as the traditional plastic card. The government plans to broaden the range of mobile IDs and introduce them for national honorees, individuals with disabilities, foreigners, and teenagers.

There are no specific laws or regulations on clean room technologies as well, but such data usage should comply to general regulations regarding collection, use, and provision of personal information.

7.7 How is location-based advertising regulated under privacy law?

The Location Information Act regulates businesses that use location information. Such businesses are classified into two categories:

- (a) **Location Information Businesses**, which collect location information and provide it to businesses offering location-based services; and
- (b) **Location-Based Service Businesses**, which provide services using location information.

To operate a location information business involving personal location information, a company must meet certain requirements, such as maintaining the necessary physical infrastructure and implementing technical and managerial measures to protect information, and must register with the KCC.

To operate a location-based service business involving personal location information, a company must file a report with the KCC, specifying its business name, principal office location, type of business, major facilities, and other required details.

Businesses processing personal location information must include the following information in their privacy policy:

- (1) The purpose of processing and the retention period for personal location information;
- (2) The legal basis and retention period for records verifying the collection, use, and provision of personal location information;
- (3) The procedures and methods for destroying personal location information; and
- (4) Details regarding the provision of personal location information to third parties.

7.8 How are data brokers defined and regulated under privacy law?

The PIPA does not specifically regulate data brokers. Instead, general provisions applicable to personal information controllers under the PIPA apply. Accordingly, if a data broker intends to trade personal data that qualifies as personal information, the broker must obtain the data subject's consent or otherwise ensure that the data has been de-identified or anonymized in compliance with the PIPA.

Separately, general regulations on data trading are set forth under the Framework Act on the Promotion of the Data Industry and Utilization. Under this Act, data trading businesses must file a report with the Minister of Science and ICT.

7.9 How is advertising to children and minors regulated under privacy law?

To process the personal information of a child under 14 years old, the consent of the child's legal representative must be obtained. Additionally, when seeking consent from the minor, the request must

be presented in a clear, simple, and easily understandable manner. The child's legal representative has the right to request access, correction or deletion, suspension of processing, and withdrawal of consent concerning the child's personal information from the data controller.

In July 2022, the PIPC issued the Guidelines on the Protection of Personal Information of Children and Adolescents, which provide detailed explanations of legal obligations and recommended practices.

The guidelines recommend that the default privacy settings for children and adolescents be set to a high level of protection, that services refrain from designing features that encourage children to provide personal information in exchange for monetary or other rewards, and that location tracking options be disabled by default. They also encourage the implementation of reasonable measures to prevent children from falsifying their age to gain unauthorized access to services. Furthermore, the guidelines advise minimizing the provision of personalized advertisements targeting children under the age of 14, and recommend that services primarily used by children avoid collecting or using behavioral information for the purpose of delivering personalized advertising.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

When a data controller makes automated decisions, it must provide data subjects with specific information about the automated decision-making process through its official website.

The information to be disclosed includes:

- (a) the fact that automated decisions are made, along with their purposes and the affected data subjects;
- (b) the types of personal information used in the automated decisions and their relevance to the decision-making process;
- (c) the considerations taken into account during the automated decision-making process, together with the procedures for processing personal information;
- (d) if sensitive information or personal information of children under the age of 14 is used, an explanation of the specific purpose and the details of the data processed; and
- (e) notification to data subjects of their right to request refusal of or an explanation concerning the automated decision-making process, including how and through what procedures such requests can be made.

When a data subject refuses the automated decision, the data controller must take action to refrain from applying the decision or reprocess the decision with human intervention.

When a data subject requests an explanation, the data controller must provide details on the results of the automated decision, the types of key personal information used, the criteria for the automated decision including the relevance of each type of personal information, and the procedures through which the key personal information was processed in the automated decision-making process.

7.11 Are there other specific advertising practices that you wish to discuss?

With respect to the use of personal information for marketing and advertising purposes, the PIPC and the KCC have issued detailed guidelines. These guidelines set forth specific requirements that companies must comply with when engaging in marketing or advertising activities involving personal information. It is important for companies to ensure that they adhere to these guidelines when conducting advertising activities.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Under the PIPA, a data controller may transfer personal information abroad only under one of the following circumstances:

- (a) When explicit consent for the transfer abroad is obtained from the data subject;
- (b) When there are specific provisions regarding the transfer of personal information abroad in laws, treaties involving the Republic of Korea, or other international agreements;
- (c) When the transfer of personal information is necessary for the conclusion and performance of a contract with the data subject, and the transfer is either disclosed in the privacy policy or communicated to the data subject;
- (d) When the recipient of the personal information has obtained certification from the PIPC, and has implemented all necessary safety measures for personal information protection and actions to ensure the protection of data subject rights, as required in the country to which the data is transferred; or
- (e) When the PIPC recognizes that the data protection system, the scope of data subject rights protection, and the remedy procedures of the country or international organization to which the personal information is transferred are effectively equivalent to the level of protection provided under the PIPA.

Data controllers must implement appropriate safeguards to protect personal information transferred abroad. If a data controller fails to take necessary measures, or if the recipient country or international organization does not provide a level of protection equivalent to that under the PIPA, the PIPC may order the suspension of the cross-border transfer.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

The transfer of personal information is categorized into two types under Korean law: ‘third-party provision’ and ‘processing entrustment’ (see question 6.1). Processing entrustment is permissible without obtaining the data subject’s consent if certain requirements are met, such as the public disclosure of relevant details in the company’s privacy policy. In contrast, third-party provision requires the explicit consent of the data subject.

If a data controller fails to properly comply with the statutory requirements, administrative fines may be imposed. The PIPC applies stricter regulatory scrutiny to the cross-border transfer of personal information compared to domestic transfers.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in South Korea? Are there minimum standards? Does this differ by sector or size of the entity?

Data controllers are required to implement technical, managerial, and physical measures to protect personal information, as outlined in the regulations. These measures include, among others, developing and enforcing an internal management plan for the secure handling of personal

information, controlling and limiting access to personal data, and utilizing encryption technologies to ensure the safe storage and transmission of personal information. The specific requirements that data controllers must comply with are detailed in the notices and guidelines issued by the PIPC.

Where a data controller processes a large volume of personal information or handles personal data of a large number of data subjects, stricter standards may apply. In particular, data controllers processing personal information of one million or more individuals are required to implement network separation measures—such as disconnecting the computers used by personnel handling personal information from the Internet—and must establish and implement procedures for managing encryption keys to ensure the safe storage of encrypted personal information.

Certain industries, including specific telecommunications providers, credit information companies, and operators of electronic databases containing medical records, are subject to more stringent or enhanced security requirements.

9.2 **How are personal data breaches regulated in South Korea? What are the requirements for notification and response?**

Under the Network Act, if a cybersecurity incident occurs, the relevant entity must report the incident within 24 hours from the time it becomes aware of the breach. The report must include details such as the date and time of occurrence, the cause of the incident, the scope of damage, and the response measures taken. The report must be submitted to either the Minister of Science and ICT or the KISA.

Separately, under the PIPA, if a personal data breach occurs, and if the breach involves sensitive information, unique identification information, results from unauthorized external access such as hacking, or affects 1,000 or more individuals, the data controller must report the breach to the PIPC or the KISA within 72 hours of becoming aware of the breach.

When a personal data breach occurs, the PIPC initiates an investigation into the circumstances and causes of the incident. If any violation of law is identified through the investigation, the PIPC may impose corrective orders, administrative fines, or other administrative sanctions.

10 **ENFORCEMENT AND PENALTIES**

10.1 **What penalties exist for non-compliance with privacy law?**

Penalties for non-compliance under the PIPA are categorized into criminal penalties, administrative surcharges, and administrative fines:

- (a) Firstly, a penalty surcharge of up to 3% of the relevant revenue may be imposed on an information and communication service provider for violating certain key privacy regulations outlined in the PIPA. Additionally, a penalty surcharge of up to KRW 500 million (approx USD 360,000) may be imposed on a data controller in the case of loss, theft, leakage, forgery, falsification, or damage to resident registration numbers under its management.
- (b) Moreover, criminal penalties of varying severity are as follows:
 - (i) Imprisonment of up to 10 years or a fine of up to KRW 100 million (approx USD 72,000) for anyone who severely disrupts the operation of public institutions by altering or deleting personal information processed by those institutions;
 - (ii) Imprisonment of up to 5 years or a fine of up to KRW 50 million (approx USD 36,000) for anyone who provides or receives personal information from a third party without obtaining the data subject's consent;

- (iii) Imprisonment of up to 3 years or a fine of up to KRW 30 million (approx USD 21,600) for anyone who obtains personal information or consent for its processing through fraud or other improper means;
- (iv) Imprisonment of up to 2 years or a fine of up to KRW 20 million (approx USD 14,400) for anyone who causes the loss, theft, leakage, forgery, falsification, or damage to personal information by failing to implement necessary security measures.
- (c) Additionally, administrative penalties include:
 - (i) A fine of up to KRW 50 million (approx USD 36,000) for collecting personal information without adhering to the proper collection/use guidelines.
 - (ii) A fine of up to KRW 30 million (approx USD 21,600) for failing to notify the data subject of required information when obtaining their consent.
 - (iii) A fine of up to KRW 20 million (approx USD 14,400) for entrusting or storing personal information overseas without informing the data subject.
 - (iv) A fine of up to KRW 10 million (approx USD 7,200) for not complying with applicable data retention requirements.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers have the right to seek damages from the data controller if they suffer losses due to the controller's violation of the PIPA, unless the data controller can prove there was no intent or negligence. The PIPA also includes a provision for punitive damages (up to five times the amount of damages incurred) in cases of loss, theft, leakage, forgery, falsification, or impairment of personal information caused by the data controller's intentional or grossly negligent actions.

Similarly, individuals can seek damages from the data controller if they incur losses due to a violation of the Credit Information Act, unless the controller can prove there was no intent or negligence. The Credit Information Act also allows for punitive damages (up to five times the amount of damages suffered) if credit information is disclosed, lost, stolen, altered, or compromised due to intentional or grossly negligent actions.

Under the Location Information Act, if a subject of personal location information suffers harm because a location information provider has violated the act, they may claim damages from the provider unless the provider can prove there was no intention or negligence involved.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Since its establishment in August 2020, the PIPC has been highly active, and the number of administrative fines and penalty surcharges imposed by the PIPC has steadily increased. In particular, when a personal data breach occurs, the PIPC actively investigates the circumstances of the incident and, upon finding violations of the law, issues corrective orders and imposes surcharges and administrative fines.

Recent notable enforcement actions by the PIPC include:

- (a) In September 2022, the PIPC imposed a penalty surcharge of KRW 69.2 billion (approx USD 50 million) on Google and KRW 30.9 billion (approx USD 22 million) on Meta for collecting users' web browsing history and app usage records without consent and using such data for online targeted advertising. Both companies were also issued corrective orders.

- (b) In November 2024, the PIPC imposed a penalty surcharge of KRW 15.1 billion (approx USD 11 million) on Kakao for a personal data breach involving its 'Open Chat' service. Kakao had assigned unencrypted temporary IDs to participants in certain Open Chat rooms by simply linking member serial numbers with chat room information. A hacker exploited this vulnerability to obtain participant information, which was then combined based on member serial numbers to create and sell a personal data file.
- (c) Also in November 2024, the PIPC imposed a penalty surcharge and administrative fine totaling approximately KRW 21.6 billion (approx USD 15.6 million) on Meta for collecting sensitive information—such as religious beliefs, political opinions, and same-sex marriage status—of approximately 980,000 South Korean users via their Facebook profiles without obtaining consent and providing such information to approximately 4,000 advertisers.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in South Korea?

There are no specific cultural considerations that uniquely impact the interpretation or enforcement of privacy laws in South Korea.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Recently, there has been a movement to amend various laws to promote the development of artificial intelligence ('AI') technologies. In the field of privacy law, amendments are being pursued to establish explicit legal grounds for processing personal data for AI development while also introducing safeguards to ensure secure management of such data. A recently proposed amendment to the PIPA introduces a special provision allowing the processing of personal information beyond the original purpose of collection for the purpose of AI development, subject to review and approval by the PIPC. The PIPC would be responsible for periodically supervising the application of this special provision and may restrict the processing if necessary.

Separately, the 2023 amendment to the PIPA introduced the 'right to data portability,' allowing data subjects to freely transfer their personal data. This provision took effect in March 2025. Under this regime, data controllers meeting certain criteria are obligated to transfer the relevant personal information upon the data subject's request. Currently, the right to data portability is applied on a limited basis during the initial phase of the system's implementation, but it is anticipated that its scope will expand over time.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Amendments to the PIPA have been driven by the need to establish a legal foundation for the active utilization of information, such as for AI development, while simultaneously protecting the rights of data subjects.

The 2023 amendment to the PIPA introduced several significant changes such as the following:

- (a) It expanded the legal grounds for the collection and use of personal data, allowing data controllers to collect and process personal information without consent when necessary for entering into or performing a contract with a data subject;
- (b) It strengthened data subject rights by introducing the right to data portability and the right to refuse or request an explanation regarding automated decision-making; and
- (c) It expanded the requirements for cross-border transfers of personal data to better align with international standards.

The 2024 amendment to the PIPA further enhanced protections by explicitly granting data subjects the right to refuse fully automated decisions and to request explanations regarding such decisions.

The 2025 amendment to the PIPA focused on strengthening the overall personal information protection framework in response to the accelerated pace of digital transformation and the rise in personal data breach incidents. The amendment introduced new standards for personal information protection in cloud environments, clarified the requirements for prior notice and consent when transferring personal data to overseas servers, and significantly raised the upper limits for penalties in cases of data breaches or mishandling of personal information. Data controllers are now required to independently assess and disclose their personal information protection systems. Furthermore, specific guidelines for the processing of personal information in AI services were established to address risks associated with AI and other emerging technologies.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

As laws and regulatory authorities impose stricter requirements on data controllers to implement enhanced protection measures, companies must pay greater attention to technical, managerial, and physical safeguards for personal information. In the event of a personal data breach, regulatory agencies may impose administrative sanctions such as penalty surcharges, and companies may also face collective actions in civil litigation. In such legal disputes, whether the data controller had implemented preventive measures prior to the incident and how the company responded immediately after the breach can significantly influence the regulatory agency's decision and the court's judgment. Accordingly, companies must establish robust response frameworks to prepare for and manage potential data breaches.

Additionally, given the recent amendments to privacy laws aimed at strengthening data subject rights—such as the introduction of the right to data portability—companies must continuously monitor legislative developments and update their personal data management systems to ensure compliance with evolving regulatory requirements.

12.3 What do you envision the privacy landscape will look like in five years?

Given the ongoing tension between the demand for stronger protection of data subject rights and the need to promote data utilization to support the development of the data industry, it is difficult to predict the precise trajectory of changes in the privacy landscape.

South Korea is known for its strict privacy regulations, but there are increasing calls for regulatory relaxation, particularly from the perspective of fostering national industries. Thus, it is possible that certain regulatory requirements may be eased in the coming years.

However, concerns over information security continue to grow, and personal data breaches remain a significant societal issue. As a result, regulatory authorities may impose even higher technical standards for data security, and enforcement actions, including sanctions, are likely to become stricter.

SWITZERLAND

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Switzerland.

The organization of the Swiss legal and court system is characterized by Switzerland's federal system. The Swiss Federal Constitution ('SFC') attributes the power to legislate in civil law matters (including civil procedure law) and criminal law matters (including criminal procedure law) to the Federation. Therefore, the core legal rules relating to privacy law are codified in Federal statutes.

The SFC provides a constitutional right to privacy in one's personal or family life and in one's home. The Swiss Civil Code ('CC') and the Swiss Federal Data Protection Act ('DPA'), for which a totally revised version came into force on September 1, 2023, put this fundamental right to privacy into concrete terms at a statutory level. Data protection provisions in Federal statutes and regulations governing sector-specific processing of personal data (eg, laws regulating the health care, pharmaceutical, financial, energy or telecoms sectors) supplement the DPA.

The 26 Cantons, the federal states of the Swiss Confederation, remain competent to legislate in administrative law matters and in the organization of their courts and administrative authorities. Each Canton has enacted its own data protection act. The Cantonal data protection Acts govern the processing of personal data by Cantonal public authorities.

1.2 What are the primary laws regulating privacy in Switzerland? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (a) The DPA is the primary law regulating data protection. It is an omnibus law governing any processing (including collection, recording, structuring, storage, disclosure, or other uses) of any personal data, ie, any information that directly or indirectly identifies an individual. It applies to the processing of personal data by businesses and organizations in all sectors of the economy as well as by federal entities.

The DPA is flanked by the Ordinance on the DPA ('DPO'). This is a governmental (Federal Council) ordinance that regulates certain aspects of the DPA more specifically, for example the minimal standards of data security or data subject rights.

Cantons regulate the processing of personal data by Cantonal and local authorities as well as by business or organizations performing tasks in the exercise of Cantonal public authority vested in them.

- (b) Sector-specific data protection and security requirements set out in laws regulating businesses and organizations in regulated sectors (eg, the health care, pharmaceutical, energy, telecom and financial sectors), provide more specific requirements applying to the processing of data. Sector-specific rules typically complement the provisions of the DPA.
- (c) Swiss data protection law is rooted in civil law's personality rights provided by the CC. In essence, the data processing principles set out in the DPA provide for protection against infringements of personality rights through excessive or otherwise unlawful use of personal data. The CC remains relevant, from a privacy law perspective, concerning libel, slander or defamation.
- (d) In addition to criminal liability governed by the DPA, a number of provisions of the Swiss Criminal Code ('CrC') are relevant in a privacy context. These include protection of a person's

reputation against defamation (including libel and slander) and criminal law provisions prohibiting unauthorized recording of private conversations or wiretapping.

- (e) Lastly, the Swiss Federal Act on Unfair Competition ('UCA'), can also be relevant in a privacy context as, for one, it provides a right of action against the disparagement of competitors and their products or services and, second, as it provides rules on mass advertising and advertising calls.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Even though many aspects of advertising are largely shaped by self-regulation, it doesn't play a particularly important role in Swiss privacy regulation, neither in general nor for advertising practices in particular.

The DPA does provide for the possibility for professional, industry and trade associations that are authorized by their statutes to protect the economic interests of their members to submit codes of conduct to the Federal Data Protection and Information Commissioner (the 'FDPIC') for comment. However, the DPA does not provide for any relevant relief or other legal consequences if a company complies with such a code of conduct (under certain conditions, the company can refrain from carrying out a so-called data protection impact assessment ('DPIA')). At the time of publication of this chapter, no codes of conduct had, to our knowledge, been submitted to the FDPIC for comment.

However, there are two pieces of self-regulation in advertising practices, that are worth mentioning:

- (a) The Principles issued by the Swiss Commission for Fairness in Commercial Communication, a self-regulatory body promoting fair trade practices in advertising and commercial communication, contain data protection and privacy-related principles. They stress the importance of the purpose limitation and transparency principles in an advertising context, but do not go beyond what the law provide to that end.
- (b) Any person in Switzerland can request that their personal postal address be added to the so-called 'Swiss Robinson List', which is maintained by the Swiss Dialog Marketing Association ('SDV'). By putting their postal address on the Swiss Robinson List, a person opts out of receiving advertising by mail and/or doorstep sales. SDV members (which include the majority of Swiss direct marketing companies) have undertaken to observe the entries in the Robinson List and the list is, in practice, also widely followed by non-members as a kind of industry self-regulation.

1.4 How is privacy law enforced in Switzerland? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

- (a) The FDPIC enforces the substantive provisions of the DPA and the DPO against businesses and organizations, as well as against Federal public authorities. According to the DPA, the FDPIC may only open an investigation ex officio or upon receipt of a complaint if there are indications of an infringement of data protection obligations under the DPA. The FDPIC has the power to issue binding decisions. It may require the respective business or organization to correct, suspend or cease certain processing of per-sonal data, or to delete personal data entirely or partially. The FDPIC may also require the business, organization or Federal authority concerned to comply with specific obligations, such as to inform individuals, grant a right of access, or to perform a data protection impact assessment. In contrast to supervisory

authorities in most jurisdictions where the GDPR is enforced, the FDPIC has not, however, the power to impose administrative fines on businesses or organizations. Nor has it the power to issue fines against individuals.

- (b) State prosecutors of the Cantons enforce criminal law provisions under the DPA against liable natural persons (and businesses under certain circumstances). State prosecutors also enforce the privacy law-related offences under the CrC and the criminal law provisions of the UCA (see question 1.2).
- (c) The data protection supervisory authorities of the Cantons enforce the Cantonal data protection Acts against Cantonal authorities or against business or organizations performing tasks in the exercise of Cantonal public authority vested in them.
- (d) Furthermore, private enforcement plays a role in the enforcement of the DPA, in particular in connection with access rights and other individual rights of data subjects. See further question 10.2.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Switzerland?

The DPA applies to the processing of personal data by any business or organization, regardless of its legal form, size or area of economic activity. It also applies to processing of personal data by natural persons in the context of business activities, but not in the context of personal (household) use.

2.2 Does privacy law in Switzerland apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The principle of effects determines the DPA's territorial scope; in other words, the DPA applies to the processing of personal data that has (or will have) effects in Switzerland, even if the processing is initiated outside of Switzerland. The term 'effect' refers to a potential or actual interference with the personality rights of a data subject in Switzerland.

This territorial scope also applies to the supervisory powers of the FDPIC.

For private enforcement actions, the Federal Act on Private International Law ('PILA') is applicable. If a place of jurisdiction can be established in Switzerland, the data subject can largely choose the law applicable to the case, which is why the DPA must be expected to apply if the data subject (or controller or another the infringing party) is located in Switzerland, even if the data processing takes place outside of Switzerland.

Controllers established outside of Switzerland have to appoint a representative in Switzerland if they regularly perform high risk and large-scale processing of personal data in connection with the offering of goods or services in Switzerland, or in connection with the monitoring of individuals' behavior taking place in Switzerland. The controller is obliged to publish the name and the address of the representative (eg, on their privacy notice).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Switzerland?

The DPA defines ‘personal data’ as any information relating to an identified or identifiable person. This includes information that directly identifies a person (eg, a full name or picture showing a person’s face) and information that allows the identification indirectly by reference to additional information (eg, email address, telephone number, social security number or customer number).

In contrast to some supervisory authorities and courts in the EU, Switzerland strictly follows the ‘relative approach’. This means that a piece of information only qualifies as personal data for those persons and organizations that have the means to establish the personal reference with reasonable effort (and also have an interest in doing so), not, however, for anyone not having those means (for more information on de-identified data, see question 3.3). It is also not enough if data only allows a person to be recognized and ‘singled out’ from the crowd, but the name or face behind the specific user cannot be found out; for this reason, IP addresses generally don’t qualify as personal data under the DPA.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The DPA considers the following categories of personal data to be ‘sensitive’:

- (a) personal data concerning religious, ideological, political or trade union-related views or activities;
- (b) personal data concerning health, the intimate sphere or the racial origin of an individual;
- (c) personal data concerning social security measures;
- (d) personal data concerning administrative or criminal proceedings and sanctions;
- (e) genetic data; and
- (f) biometric data that uniquely identifies an individual.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under Swiss privacy law, the treatment of anonymized, pseudonymized, and de-identified data involves nuanced distinctions with significant legal implications. The term ‘de-identified data’ serves as an umbrella term, encompassing both anonymization and pseudonymization.

For data to qualify as ‘anonymized’ all identifiers (eg, name, address, date of birth) must be irreversibly masked or deleted, ensuring no re-identification is possible without disproportionate effort. Once anonymized, the data no longer falls under the scope of the DPA and data protection obligations no longer apply. The anonymization of data is considered to be an equivalent to the deletion of data.

‘Pseudonymization’, on the other hand, replaces direct identifiers with pseudonyms, allowing re-identification for anyone with access to the pseudonymization key (eg, a reference list linking the pseudonyms to the names of the data subjects). For parties without access to the pseudonymization key, the data is treated as anonymized and not subject to the DPA. The Zurich Commercial Court has ruled that pseudonymization’s legal status depends on the recipient’s ability to re-identify individuals. For example, data transferred to a foreign authority without the key may be considered anonymized, even if re-identification is theoretically possible through judicial assistance.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The following principles set out in the DPA are the key obligations that controllers need to follow regarding their processing of personal data:

- (a) lawfulness;
- (b) fairness and transparency;
- (c) purpose limitation;
- (d) proportionality (data minimization and storage limitation);
- (e) accuracy; and
- (f) security (integrity, confidentiality and availability).

Moreover, where consent from the data subject is required, this must be given voluntarily after comprehensive information (informed consent).

This doesn't mean, however, that consent (or any other legal basis) is required for all processing activities (for more information, see question 4.3).

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The DPA distinguishes between controllers and processors.

- (a) The term 'controller' is defined as a private person (business, organization, natural person etc) or Federal authority that determines (alone or jointly with others) the purpose and means of the processing of personal data. Controllers are primarily responsible for ensuring compliance with the DPA.
- (b) 'Processors' are businesses, organizations, natural persons or Federal authorities who process personal data solely on behalf of the controller. Even if the controller is responsible to the data subject for the lawfulness of the processing of their data and compliance with the DPA in general, the DPA also sets out legal obligations applying directly to the processor (including data security obligations, restrictions on engaging sub-processors and the requirement to maintain records of processing activities).

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Under the DPA, not all data processing activities require a legal basis, unlike the GDPR. A (private) controller only needs to show 'justification' (consent, law or an overriding personal or public interest) in the following cases:

- (a) personal data is processed in violation of one of the key obligations (see question 4.1);
- (b) personal data is processed contrary to the express will of the data subject; or
- (c) 'sensitive' personal data (as described in question 3.2) is disclosed to a third party.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The DPA provides for the following list of minimum information that must be communicated to data subjects (eg, in the privacy notice) each time data is collected, regardless of whether the data is collected and processed for advertising or other purposes:

- (a) identity and contact information of the controller (including their Swiss representative if one is appointed (see question 2.2));
- (b) purpose of the data processing;
- (c) recipients or categories of recipients to whom personal data is disclosed
- (d) if personal data is transferred outside of Switzerland, the controller needs to state the countries to which the controller intends to disclose personal data (the indication of regions such as 'EU' or even 'worldwide' suffices) and, if the recipient country doesn't offer an adequate level of data protection, state which safeguards (eg, standard contractual clauses) or derogations (eg consent in an individual case) are in place; and
- (e) if personal data is not collected from the data subject, the categories of personal data also needs to be communicated (the controller may freely choose the categories into which the personal data should be grouped, and how to label the categories (eg, by saying 'contact data' is collected, rather than 'email address, phone number and postal address')).

At a first glance, this list seems to be very short, especially when compared to the relevant provisions in the GDPR. However, the list is not exhaustive, as the DPA states that the controller needs to provide the data subject with all information required so that they can assert their rights under the DPA and to ensure that the processing of personal data is transparent at the time of collection. Therefore, it is customary to provide data subjects with additional information (eg, in a privacy notice), such as information about their rights as data subject or even retention periods. Again, this information needs to be provided regardless of whether the data is collected and processed for advertising or other purposes.

Apart from the provisions of the DPA, there are additional information obligations that are relevant in the context of advertising, such as when cookies or similar technologies are used (see question 7.2) or in cases of mass advertising sent by telecommunications (see question 5.3). This information can be included in the privacy notice (which is often done), but doesn't have to be.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Data subjects have a right to:

- (a) request information about the processing of their personal data (right to access);
- (b) have incorrect personal data corrected;
- (c) request the deletion of personal data;
- (d) object to the processing of their data;
- (e) request the disclosure of certain personal data in a commonly used electronic format or its transfer to other controllers; and
- (f) revoke their consent with effect for the future (where processing is based on consent).

These rights of individuals are subject to conditions and exceptions. For example, the right of access may be limited, deferred or denied to the extent necessary to protect the privacy interests of other data subjects or the legitimate interests of the controller or third parties that override the data subject's privacy interests.

In an advertising context, the right to object (and the right to invoke consent, which is, in effect, an objection) plays a major role (even if the other rights are applicable as well, given that the relevant conditions are met). Data subjects can exercise this right at any time and do not have to give a reason for objecting. If a data subject asserts this right, a controller must comply with the objection, as further processing of the personal data for marketing purposes would only be possible if there were a justification (see question 4.3), which is generally not available in such cases (lack of a legal basis or consent and the existence of an overriding interest is difficult to argue for marketing purposes).

In the realm of email marketing, explicit, informed consent ('opt-in') is mandatory before sending promotional materials to non-clients, and data subjects must be given the ability to easily withdraw this consent. For more information, see question 5.3.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

- (a) Consent (or other 'justification', such as an overriding interest) is generally not required to process personal data for marketing purposes, nor is it required to perform profiling (whether or not high risk) (see question 7.10) or for the disclosure of personal data to a third party (eg, so that the third party can use the data for their own marketing purposes). This is subject to the condition that:
 - (i) the data subject was sufficiently informed in the privacy notice during the collection of their personal data that their data would be used for marketing purposes (including profiling, if applicable) and/or that it would be disclosed to third parties so that they could process it for their own marketing purposes;
 - (ii) the processing of personal data for marketing purposes is not disproportionate (an example of where consent is likely to be required is where a publisher creates comprehensive profiles of its registered users that go beyond the assignment to individual interests); and
 - (iii) no particularly sensitive personal data, such as health data, is disclosed to the third party.
- (b) There are different rules for email marketing, which are not rooted in the DPA, but rather in the UCA:
 - (i) The sending of unsolicited mass direct marketing emails (or other forms of electronic communications, eg, WhatsApp, SMS) to non-clients is only permitted if the recipient has provided their prior opt-in consent;
 - (ii) To be valid, consent must be given voluntarily after adequate information has been provided ('informed consent'), ie, the data subject must be informed that their email address will be used for marketing purposes and must have consented to such use. It is not permissible to obtain consent by sending unsolicited mass communications asking for such consent (as this communication itself constitutes marketing). Swiss law is, however, less strict than EU law with regards to how consent is obtained. For example, a consent box can be pre-ticked and double opt-in is also not required;

- (iii) Opt-in consent is exceptionally not necessary if, cumulatively:
 - the sender received the contact information of the recipient in the course of a sale of its products or services (ie, a contract must be formed—opening a customer account is generally not considered to be sufficient if it does not lead to the conclusion of a contract);
 - the recipient was informed at the time of collection of the opportunity to opt out of the use of their contact information for advertising purposes (eg, by a privacy notice); and
 - the mass advertising relates to similar products or services of the sender.
- (iv) Regardless of whether opt-in consent is required or not, each marketing communication must identify the sender and provide an easy and free way to opt-out of receiving future such communications (usually through an unsubscribe link at the bottom of each email).

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The general framework described above applies to the use of vendors and other third parties. Sensitive personal data may only be disclosed to third parties in their capacity as controllers if:

- (a) the data subject has consented to the processing;
- (b) Swiss (federal, cantonal or municipal) law provides for such processing; or
- (c) an overriding private or public interest justifies such processing.

Prior approval from the controller is required for subcontracting.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The answer to this question depends on the role in which a vendor or other third party processes the data:

- (a) If the vendor or other third party receives the personal data to process it on behalf and for the purposes of the company (acting as the controller), it qualifies as a processor. The controller-processor relationship needs to be governed by a contract (when not established by law).

Even if the DPA doesn't provide a list of minimum requirements that the contract needs to cover, it is customary to adhere to the standard required by Article 28 of the GDPR (with a few amendments for Swiss law). As such, data processing agreements under Swiss law generally contain the following:

- (i) A clear definition of the scope and the processing purpose as well as the data categories that are being processed;
- (ii) The controller's right to instruct (which also applies to the disclosure of personal data abroad) and processor's obligation to process the personal data only based on these documented instructions;
- (iii) The obligation for the processor to maintain confidentiality;
- (iv) Technical/organizational security measures;
- (v) The requirement of prior (general or specific) approval from the controller for subcontracting;

- (vi) A breach notification where processors inform controllers of data breaches without undue delay;
- (vii) The obligation of the processor to support the controller in the implementation of and compliance with the DPA (eg, by providing information the controller needs for fulfilling its own documentation and due diligence obligations);
- (viii) Audit rights of the controller; and
- (ix) Post-termination obligations: data must be returned or deleted after the contract ends.

Even if GDPR-compliant data processing agreements can be used for the purposes of Swiss data protection, it is recommended to add references to the Swiss DPA (in addition to the GDPR), to ensure that data exports from Switzerland (in addition exports from the EU) are also covered and that the EU Standard Contractual Clauses (if required and used) are amended for compliance with the DPA.

- (b) In cases where the vendor or other third party qualifies as a ‘controller’, the following two scenarios need to be distinguished:
 - (i) If the company and the vendor or other third party jointly determine the purpose and the means of a processing activity, they are ‘joint controllers’. An example in the context of (online) marketing is the following: A publisher embeds a 3rd party cookie of the advertiser on its website so that the advertiser can use it to collect user data and display its advertising to users. In this scenario, the parties are regularly qualified as joint controllers regarding the embedding of the cookie and the associated data collection, at least if the publisher co-controls the parameters of this data collection (eg by co-determining from which users personal data is collected). The GDPR stipulates that joint controllers must conclude a ‘joint controllership agreement’ (‘JCA’). Although the DPA does not contain an explicit obligation to conclude a JCA (in contrast to the GDPR), it is also common practice in Switzerland to conclude one if the requirements for a joint controllership are met. This JCA must specify which of the Controllers involved will act externally and, for example, respond to requests from data subjects or comply with information obligations.
 - (ii) If the company discloses the personal data to the vendor or other third party so that the latter can (also) process it for its own purposes, then the vendor or other third party is also solely responsible for compliance with data protection in this context. For such a controller-controller transfer, neither the GDPR nor the DPA stipulate that a contract must be concluded (as long as both parties are located in a country with adequate data protection; see question 8). However, even in a situation of controller-controller transfer, it is often advisable to conclude a contract specifying the purposes for which the receiving service provider may process the data and that it must keep the data confidential.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

The general framework described above applies to due diligence measures companies are expected to undertake in their privacy practices.

According to the DPA, a data protection impact assessment (‘DPIA’) must be carried out if a planned data processing operation may result in a high risk to the personality or fundamental rights of the data

subject. This high risk arises, particularly when using new technologies, from the nature, scope, circumstances, and purpose of the processing. It is notably present when processing particularly sensitive personal data on a large scale or when systematically monitoring extensive public areas.

The DPIA must describe the planned processing activity, assess the risks for the data subjects associated with it, and define protective measures. Multiple similar processing operations may be assessed jointly. Should the company, in the course of the DPIA, come to the conclusion that the planned processing activity will still result in a high risk to the personality or fundamental rights of the data subject despite the protective measures envisaged by the controller, the controller must obtain the prior opinion of the FDPIC.

There are exemptions to the obligation to perform a DPIA, such as if the controller is legally obligated to process the data.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The general framework described above applies to direct marketing communications, including email, texts, and push notifications. In addition to the data protection requirements set out in the DPA, the provisions of the UCA that require an opt-in or opt-out for mass communication (eg, newsletters or other emails sent at once to a very large number of recipients) need to be complied with (see question 5.3).

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

There is no cookie law or similar law that governs the use of cookies, pixels or similar. The general framework described above applies to the collection of personal data by use of tracking technologies.

It is not necessary to obtain consent for the use of cookies and similar tracking technologies (regardless of the purpose for which they are used and whether they are 1st or 3rd party cookies). The relevant provision cannot be found in the DPA, but rather in the Telecommunications Act.

Still, the user must be informed in advance about the use of cookies if they qualify as personal data from the company's point of view (ie, they allow the company, such as a publisher, to identify the user, see question 3.1), which can be done via the privacy notice, a cookie policy or a cookie banner. Additionally, the user must be provided with an option to object (this can be cookie consent management, but in the simplest form it is also sufficient to inform the user that they can also block cookies in their browser). This is in contrast to the position in the EU, where the ePrivacy Directive requires that users must consent to all cookies that are not technically necessary for the operation of the website.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific laws in Swiss privacy law that regulate loyalty programs and promotions and the general framework described above applies. The FDPIC has in the past closely scrutinized the information provided in privacy policies concerning loyalty programs.

7.4 How is social media and influencer marketing regulated under privacy law?

There are no specific laws in Swiss privacy law that regulate social media and influencer marketing, and the general framework described above applies. Advertisers should inform data subjects in their privacy notices about their social media marketing activities.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are no specific laws in Swiss privacy law that regulate targeted and personalized advertising and the general framework described above applies.

The obligations of the DPA concerning profiling require special attention (see question 7.10).

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific laws in Swiss privacy law that regulate digital identity resolution and clean room technologies and the general framework described above applies.

7.7 How is location-based advertising regulated under privacy law?

There are no specific laws in Swiss privacy law that regulate location-based advertising and the general framework described above applies. However, it is important to notice the landscape around cookies and direct marketing by email and by telephone.

7.8 How are data brokers defined and regulated under privacy law?

There are no specific privacy rules governing data brokers and the general framework described above applies (see, in particular, question 6.1).

7.9 How is advertising to children and minors regulated under privacy law?

There are no specific provisions in the DPA that regulate the processing of children's or minors' personal data and the general framework described above applies (in general and for advertising purposes in particular).

However, the relevant provisions of the CC need to be observed. Here, a distinction is made between children who themselves are able to assess the consequences of the processing of data (rule of thumb: 13 and older) and other (younger) children, who are not yet capable of such judgement. A child capable of judgment can, for example, validly consent (where such consent is necessary) to receiving marketing communication and having its personal data processed for such purposes. This means also, that a privacy notice (or other information) has to be made available to a child capable of judgement. If a child is not yet capable of judgement, only their parents or other competent custodian can give valid consent for them and a privacy notice has to be made available to them (and not the child).

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific privacy rules governing the use of artificial intelligence and the general framework described above applies.

However, the DPA specifically regulates the concepts of ‘profiling’ and ‘automated decision-making:

- (a) ‘Profiling’ occurs when a person’s personal data is used to evaluate them according to certain personal aspects, whereby this evaluation is carried out automatically—ie by a computer, not by a person. Profiling thus describes a processing procedure that is intended to recognize patterns that allow conclusions to be drawn—for example, about the possible behavior, abilities, interests or health of a person or a specific group of people.

An example of profiling would be when a publisher tracks a user’s behavior on its website to be able to draw conclusions about their interests based on their behavior patterns. The evaluation of behavioral patterns could lead to conclusions about a person’s interests, which can then in turn be used to display personalized advertising. However, if the publisher simply divides the users registered on its website into age or gender to analyze the demographic distribution, this does not constitute profiling, as there is no evaluation of personal characteristics. Conversely, profiling does not necessarily have to result in a ‘profile’.

If, on the other hand, profiling leads to data being linked in such a way that they provide a picture of the essential characteristics of a data subject and this ‘profile’ is stored and also entails an increased risk to personal rights, then this is qualified as a ‘high-risk profiling’ under the DPA. A high-risk profiling is, in other words, a profiling that results in a personality profile (and is therefore to be regarded as ‘sensitive’).

However, the distinction between normal profiling and high-risk profiling has hardly any factual or legal consequences. The only exception in the area relevant here is that, in the case of high-risk profiling, consent must be expressly obtained, if such consent must be obtained at all (see question 4.3), and a DPIA must be carried out (see question 6.3). That said, the fact that the data processing—whether with or without profiling—is particularly far-reaching may of course qualify it as ‘disproportionate’ and therefore require consent or another justification.

- (b) An automated individual decision, on the other hand, is defined as a decision based solely on automated processing (‘automated decision-making’). If this decision has legal consequences for the data subject or significantly affects them, the data subject must be informed of the automated decision-making and that they have the right to have the decision reviewed by a human being.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The restrictions on transfers to third countries are comparable to those under the GDPR: a transfer of personal data is only permitted to recipients in countries that provide for an adequate level of data protection. The Federal Council publishes a list of countries that, according to its assessment, provide an adequate level of data protection. This list is binding.

Personal data may only be transferred to countries without an adequate level of data protection if there are either sufficient safeguards in place to compensate for such lack of protection, or if one of the derogations defined in the DPA applies:

- (a) The DPA provides for the following safeguards:
 - (i) standard contractual clauses issued, approved or recognized by the FDPIC (the EU Standard Contractual Clauses, with a few Swiss amendments, have been approved by the FDPIC);
 - (ii) binding corporate rules approved by the FDPIC or another competent data protection supervisory authority in a country that provides adequate protection;
 - (iii) (subject to prior notification to the FDPIC) contractual clauses between the controller or processor and the recipient of the personal data abroad; and
 - (iv) international treaties to which Switzerland is a party.
- (b) Under the following derogations, personal data may also be transferred to a country without an adequate level of data protection without having to implement one of the above-mentioned safeguards:
 - (i) the data subject has expressly consented to the disclosure;
 - (ii) the disclosure is directly related to the conclusion or execution of a contract:
 - between the Controller and the data subject, or
 - between the Controller and its contractual partner in the interest of the data subject;
 - (iii) the disclosure is necessary for:
 - the protection of an overriding public interest, or
 - the establishment, exercise or enforcement of legal claims before a court or other competent foreign authority;
 - (iv) the disclosure is necessary to protect the life or physical integrity of the data subject or a third party and it is not possible to obtain the data subject's consent within a reasonable period of time;
 - (v) the data subject has made the data generally accessible and has not expressly prohibited processing; or
 - (vi) the data originate from a register provided for by law, which is accessible to the public or to persons with a legitimate interest (eg commercial register, land register etc) provided that the legal requirements for access are met in the individual case.

It should be noted that the EEA countries are considered to be third countries (even though these are countries providing an adequate level of data protection, which is why there is no need for additional safeguards or the reliance on derogations).

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

For the purposes of the DPA, companies within a group of companies are considered as third parties. Hence, a transfer to another company within a group constitutes a disclosure to a third party.

Where personal data is transferred to a group company in a country without adequate level of protection, appropriate safeguards need to be put in place (eg, binding corporate rules or standard contractual clauses entered into by the group companies).

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Switzerland? Are there minimum standards? Does this differ by sector or size of the entity?

There is no uniform data security law. A number of sector-specific laws and regulations (eg, in the energy, banking and health care sectors) regulate aspects of data or information security. The DPA and the DPO define a standard for the security of personal data (see question 3.1). Controllers (and also processors!) are required to ensure data security that is appropriate to the risk (of the relevant processing activity) through the implementation of technical and organizational measures.

The DPO sets out a minimum standard: To ensure an appropriate data security, the controller and processor must determine the protection requirements of the personal data at issue according to the type of data and the purpose, nature, scope and circumstances of the processing. Whether the technical and organizational measures are appropriate, needs, in turn, to be assessed with regard to these requirements and by considering also the state of the art and the implementation costs.

The DPO sets out the protection goals that are to be pursued with the technical and organizational measures, namely ensuring that the data:

- (a) is only accessible to authorized persons (confidentiality);
- (b) is available when they are needed (availability);
- (c) isn't modified without authorization or unintentionally (integrity);
- (d) is processed in a traceable manner (traceability).

9.2 How are personal data breaches regulated in Switzerland? What are the requirements for notification and response?

Under the DPA, controllers are required to notify the FDPIC of personal data breaches that may result in a high risk for data subjects. There is no fixed deadline, the notification has to happen 'as soon as possible', meaning without undue delay. In their notification, they will need to address the type of personal data breach, its consequences, and the measures taken or planned to remedy the breach and mitigate risks for data subjects.

Controllers are required to notify the data subjects affected by the personal data breach if such notification is necessary in order to protect the data subjects or if the FDPIC so requests. Processors who detect a personal data breach are required to notify the controller of the breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The FDPIC does not have the right to issue administrative fines. The state prosecutors enforce the criminal law provisions of the DPA.

Currently, the DPA provides that private individuals may be fined up to CHF 250,000 (approx USD 300,000) if they are responsible for the violation of specific information and notification requirements under the DPA (eg, willfully providing false or incomplete information in response to a data subject access request, willful failure to ensure there are sufficient guarantees for international data transfers, or willful failure to comply with minimum data security requirements).

The DPA recognizes the criminal liability of businesses and organizations. The responsible individuals will primarily be liable. Who can be sanctioned as a responsible person results from a legal obligation to ensure compliance with the DPA within the company (eg someone in a managerial position) or from the fact that a person is responsible for managing the relevant data processing process (without having to be part of an executive body). However, the business or organization (controller or processor) may be held liable for a fine of up to CHF 50,000 (approx USD 60,000) if determining who, in the organization, is responsible for the infringement would require disproportionate investigative efforts.

10.2 Do consumers have a private right of action? What remedies are available to them?

- (a) The CC provides for private rights of action against infringements of personality rights. The following remedies are available:
 - (i) prior restraints and other pre-publication injunctions;
 - (ii) removal of an existing infringement (this may include a right to be forgotten);
 - (iii) a declaratory judgment (if the effect of the infringement is continuing); and
 - (iv) claims for compensatory damages, moral damages, and disgorgement of profits.
- (b) The DPA provides private rights of actions against infringements of personality rights protected under the DPA. Of particular practical relevance is litigation concerning the exercise of the rights of access, rectification and deletion. Yet data subjects may also claim infringement of key data privacy principles such as purpose limitation, data minimization and data security. The remedies set out in the CC apply by analogy to such claims.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Privacy enforcement in Switzerland has become more active in recent years, particularly since the implementation of the revised DPA. For example, the FDPIC has newly gained expanded powers to investigate and issue administrative measures for data protection violations.

We are aware of one recent investigation of the FDPIC in relation to an advertising context. The investigations were directed against a well-known online marketplace. The FDPIC concluded that the privacy notice of this online marketplace did not contain sufficient information about the use of personal data, especially for personalized advertising, and disclosure of data to third parties (or rather, one large media group in particular) in several respects. The FDPIC issued a total of 11 recommendations in its final report. Inter alia, the FDPIC recommended that the marketplace make it more transparent to users as to which justifications it relied when processing personal data. This recommendation is problematic in two ways: For one, in Switzerland a justification isn't required for every processing activity (see question 4.3). Second, even if a controller has to rely on a justification for a specific processing activity, it is not required to inform the data subjects about this justification. This recommendation (among others) was, therefore, highly criticized in public. It must be noted that the investigation was opened under the old DPA (in 2017) and, as such, the recommendations are based on the old law, even if the final report were published after the new DPA came into force. Also, the recommendations of the FDPIC are non-binding.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Switzerland?

No.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

Concerning the general hot topic of profiling, the DPA includes a definition for profiling ‘involving a high risk’, which, in essence, is a profiling that results in a personality profile, and thus bears a high risk of negative consequences for the data subject. However, for private industry, the relevance of both terms is rather minimal; there is a limitation on credit rating agencies using profiling involving a high risk and, insofar as a controller relies on consent in order to conduct a profiling involving a high risk, the consent must be explicit.

In addition to programmatic advertising, other hot topics are voice and facial recognition and monitoring of data subjects’ behavior online or in public spaces, as well as data and cyber security.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Data-driven business models have become prevalent in recent years. Consumers acknowledge the value of these business models, but are also increasingly concerned about their privacy in a digital economy. In particular, decision-making based on algorithms and big data analysis creates a perception of losing control over one’s personal data. In the wake of various high-profile data breaches, information security has become an important topic. It is no longer left to the IT departments of companies and public institutions, but, rather, an ongoing obligation that has become part of board and C-level management duties. In addition, legislative developments in the EU and in Switzerland have raised awareness for data privacy by both consumers and companies. Triggered by these changes, data privacy has been established as a topic of increasing priority of the top management of companies over the past few years.

With the rise of artificial intelligence and the plethora of new business models growing out of it, the privacy landscape will have to grapple with the question of how to utilize data to find out information and feed such technologies, while remaining in compliance with regulatory rules.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

It has become increasingly challenging for businesses to comply with high data privacy standards while retaining their competitive edge. Multi-layered governance of the processing of personal data (by European, Federal and Cantonal laws and regulations) and multi-layered enforcement (see questions 10 and 12.3) complicate compliance.

In an advertising context, providing the notices and controls to data subjects that revised data privacy laws require often proves difficult. Where advertisers do not have a direct business relationship with their target audience, they will need to rely on publishers and intermediaries to that end. Furthermore, the nature of the relationship between advertisers and providers of customer matching services or other intermediaries as joint or separate controllers, or controller-processor relationships, will likely continue to be debated. It will remain unresolved until case law is more developed and adopted in a Swiss law context under the DPA. Meanwhile, data-driven businesses (including businesses in the online media and advertising industries) will have to develop targeting measures that take into account the concerns of regulators and the public at large, eg, by developing effective anonymization measures and advertising identifiers that cannot be traced to individuals.

12.3 What do you envision the privacy landscape will look like in five years?

In five years, Switzerland's privacy landscape will likely be significantly influenced by the integration of artificial intelligence. Sector-specific regulations, particularly for high-risk areas like healthcare and finance, will probably become more prevalent, complementing the existing DPA. Switzerland's announced ratification of the Council of Europe's AI Convention will necessitate legislative amendments, emphasizing transparency and accountability in AI systems. Public awareness of AI-related privacy concerns will probably increase, which might lead to stricter enforcement of data protection regulations and more rigorous compliance requirements for organizations.

In general, the public's awareness of data and privacy will likely increase in the next few years. Also, it may be expected that data protection and security provisions in sector-specific laws and regulations concerning data uses in highly regulated sectors will continue to receive more attention. Switzerland will likely implement targeted regulations for high-risk sectors like healthcare, finance, and autonomous vehicles, ensuring both flexibility and accountability.

This means that companies of all sizes will be faced with data compliance questions. So, while privacy laws might be a tad enigmatic or even burdensome to companies at this point, businesses will learn to trust the DPA in the next few years, making it an increasingly familiar and appreciated part of business regulation—something we observe when advising our clients as well.

Private enforcement remains costly due to limited pre-trial disclosure, and because opportunities for collective legal action are very limited. The effectiveness of enforcement by the FDPIC depends significantly on the resources made available to it, which remain rather limited. The revised DPA newly empowers the FDPIC to issue binding decisions and require controllers and processors to change their data processing operations. Still, without the power to issue fines, and with limited resources, the effects of enforcement by the FDPIC on the privacy landscape may remain rather limited. Finally, state prosecutors tend to have other enforcement priorities and a lack of sufficient data privacy know-how. Enforcement of the criminal law provisions of the DPA, therefore, may remain rather limited too.

TRINIDAD AND TOBAGO

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Trinidad and Tobago.

The Constitution of Trinidad and Tobago recognizes and enshrines the rights of individuals to respect for their private and family life.

The main statute regulating privacy in Trinidad and Tobago is the Data Protection Act (Chap 22:04). The object of this Act is to ensure that protection is afforded to an individual's right to privacy and the right to maintain sensitive personal information as private and personal. However, as at July 2025, the Data Protection Act is only partially in force.

1.2 What are the primary laws regulating privacy in Trinidad and Tobago? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy is regulated by the following:

- (a) Section 4 of the Constitution which enshrines the rights of individuals to respect for their private and family life as a fundamental human right in Trinidad and Tobago;
- (b) The Data Protection Act which sets out the General Privacy Principles in respect of the handling, storage or processing of personal information belonging to another person; and
- (c) The Interception of Communications Act (Chap 15:08) which generally prohibits the interception of private communications transmitted between persons.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation remains the primary mechanism for ensuring responsible advertising practices in Trinidad and Tobago, because the Data Protection Act has only been partially enacted and the substantive provisions governing the protection of personal information are not yet in force.

The Trinidad and Tobago Standard, Advertising—Part 1: General Requirements (3rd Revision) TTS 94-1:2017 ('the Advertising Standard') (see question 5.2), although not compulsory, is generally adhered to in Trinidad and Tobago as best practice. Therefore, self-regulation plays a substantial role in privacy protection in advertising, filling the gap left by the incomplete enactment of the Data Protection Act.

1.4 How is privacy law enforced in Trinidad and Tobago? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

As at July 2025, the Data Protection Act is only partly in force. Thus, notwithstanding the existence, and coming into force, of the General Privacy Principles, the specific provisions contained in the Act for the protection of personal data and personal information requested, collected and stored by both public bodies and the private sector, by inter alia requiring that they (a) follow the General Privacy Principles and (b) obtain the consent of individuals prior to disclosing their personal information to a party residing in another jurisdiction, are not yet in force. Nor, indeed are those relating to enforcement.

As well as the General Privacy Principles, other provisions of the Data Protection Act which are in force include the establishment of the Office of the Information Commissioner, headed by an Information Commissioner who is responsible for monitoring the administration of the Act to ensure its purposes are achieved. However, as at July 2025, the Office of the Information Commissioner has not been staffed and no Information Commissioner has been appointed.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Trinidad and Tobago?

Upon the proclamation of all of the provisions of the Data Protection Act, all entities in the private sector of Trinidad and Tobago (including companies) will be subject to the Data Protection Act.

2.2 Does privacy law in Trinidad and Tobago apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Generally, there is a presumption of statutory interpretation that legislation applies only to conduct taking place within the territory, unless the legislation specifically indicates that it has extra-territorial effect. There is no indication in the Data Protection Act that it imposes obligations on companies outside of Trinidad and Tobago to protect the privacy of individuals in Trinidad and Tobago.

Note, however, that the General Privacy Principles (see question 4.1) include the requirement that personal information which is requested to be disclosed outside of Trinidad and Tobago must be regulated, and comparable safeguards to those under the Data Protection Act must exist in the jurisdiction receiving the personal information. Section 46 of the Data Protection Act (though not in force as at July 2025) regulates when, and the manner in which, a public body may disclose personal information under its custody and control to a party residing in another jurisdiction. However, these obligations rest on the persons in Trinidad and Tobago who handle, store or process personal information belonging to another person.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Trinidad and Tobago?

The Data Protection Act defines ‘personal information’ as information about an identifiable individual that is recorded in any form including:

- (a) information relating to the race, nationality or ethnic origin, religion, age or marital status of the individual;
- (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to the financial transactions in which the individual has been involved or which refers to the individual;
- (c) any identifying number, symbol or other particular designed to identify the individual;
- (d) the address and telephone contact number of the individual;
- (e) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;

- (f) correspondence sent to an establishment by the individual that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence which would reveal the contents of the original correspondence;
- (g) the views and opinions of any other person about the individual; or
- (h) the fingerprints, DNA, blood type or the biometric characteristics of the individual.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Data Protection Act also refers to ‘sensitive personal information’ which is defined as meaning information on a person’s:

- (a) racial or ethnic origins;
- (b) political affiliations or trade union membership;
- (c) religious beliefs or other beliefs of a similar nature;
- (d) physical or mental health or condition;
- (e) sexual orientation or sexual life; or
- (f) criminal or financial record.

The General Privacy Principles contained in the Data Protection Act include the requirement that sensitive personal information be protected from processing except where otherwise provided for by written law (see question 4.1). Further, other sections of the Data Protection Act (which are not yet in force) provide certain limitations on the processing of sensitive personal information in the possession of a public body or corporation.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

The Data Protection Act does not expressly address anonymized, pseudonymized or de-identified data. However, based on the definition of ‘personal information’, which refers to information about an ‘identifiable individual’, the treatment of such data will depend, in our view, on whether re-identification is possible. Thus:

- (a) **Anonymized data:** if the data has been fully anonymized, meaning that all identifiers have been removed and cannot trace back to the individual, it may fall outside the scope of the Data Protection Act, as it no longer pertains to an ‘identifiable individual’;
- (b) **Pseudonymized data:** if data has been altered to remove direct identifiers but can still be linked back to an individual through further information, it may still be considered personal information under the Data Protection Act; and
- (c) **De-identified data:** if the data can be re-linked to the individual using additional information, then it may fall within the scope of the Act. However, if de-identification is irreversible, the data may no longer be subject to protection.

As the Data Protection Act does not specifically regulate anonymized, pseudonymized and de-identified data, best practices should be followed to ensure that such data remains protected where necessary. Additionally, corporations handling such data should assess the risk of identification/re-identification and adopt appropriate safeguards, particularly in industries handling sensitive personal information.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Under the Data Protection Act, companies handling personal information are required to follow the General Privacy Principles. These are:

- (a) an organization shall be responsible for the personal information under its control;
- (b) the purpose for which personal information is collected shall be identified by the organization before or at the time of collection;
- (c) knowledge and consent of the individual are required for the collection, use or disclosure of personal information;
- (d) collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization;
- (e) personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual;
- (f) personal information shall be accurate, complete and up-to-date as is necessary for the purpose of collection;
- (g) personal information is to be protected by such appropriate safeguards having regard to the sensitivity of the information;
- (h) sensitive personal information is protected from processing except where otherwise provided for by written law;
- (i) organizations are to make available to individuals documents regarding their policies and practices related to the management of personal information except where otherwise provided by written law;
- (j) organizations shall, except where otherwise provided by written law, disclose at the request of the individual, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information;
- (k) the individual has the ability to challenge the organization's compliance with the above principles and receive timely and appropriate engagement from the organization; and
- (l) personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

The Data Protection Act provides that when transferring personal data outside of Trinidad and Tobago, companies must inform individuals of the purpose of the transfer, the identity of the requesting party, and the relevant data protection authority in the receiving jurisdiction. Disclosures to third parties are generally limited except with the consent of the individual. Please note that while these provisions are not yet in force, they represent best practice in Trinidad and Tobago.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

There is no distinction in the Data Protection Act between a controller and a processor of personal information. In particular, a person who collects, retains, manages, uses, processes or stores personal information or uses an intermediary or telecommunications service provider located in Trinidad and Tobago to provide any of the above services, will be subject to the General Privacy Principles set out in the Data Protection Act, once the underlying provision giving rise to this obligation is in force.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The Data Protection Act requires that personal data be processed in a lawful manner. Consent is explicitly required for the collection, use or disclosure of personal information (see General Privacy Principle (c) at question 4.1). This requirement is reinforced by provisions (not yet in force) whereby personal data under a company's control must not be disclosed to a third party without the consent of the individual except where required by law, court order or for the original purpose of collection. Further, a company may not process sensitive personal information unless it obtains the prior consent of the individual.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Under the Data Protection Act, companies that process personal information for advertising purposes should provide clear and transparent privacy notices that inform individuals about the purpose for which their personal information is being collected and how their data is collected, used, and stored. Based on the General Privacy Principles (for which see question 4.1), the following information should be included, without limitation:

- (a) **identity of the company:** the name, contact details and registered office of the company collecting the data;
- (b) **purpose of processing:** a clear explanation that personal information is being processed for advertising purposes, including how it will be used for example, targeted marketing, analytics, etc;
- (c) **consent:** a clear explanation that, by submitting the personal information, the individual consents to the processing of the same for the purpose identified;
- (d) **description of data to be collected:** a list of the categories of personal data collected, such as names, contact details etc;
- (e) **retention period:** an indication of how long the data will be retained before being deleted;
- (f) **opt-out mechanisms:** details on how individuals can withdraw consent;
- (g) **access to any additional company policies or practices:** identification of where the individual can access the company's privacy policies; and
- (h) **contact information:** instructions on how individuals can contact the company for data privacy inquiries, complaints or requests related to their personal information.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the right to transparency regarding how their personal information is collected, used and disclosed for advertising purposes. General Privacy Principle (b) provides that companies must identify the purpose for which personal information is collected. Consent is a key requirement under General Privacy Principle (c), in which consumers' knowledge and consent are required before their personal data can be collected, used or disclosed. Consumers also have the right to access and correct their personal data: General Privacy Principle (j). As to the General Privacy Principles see question 4.1.

The Advertising Standard prohibits the portrayal or referral to a person or a person's identifiable property in advertisements without the permission of the individual or owner concerned, except where the person or the person's specific identifiable properties are in the public domain. The Advertising Standard also generally requires that permission first be obtained before pictorial or other representations of persons are used in advertisements.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under General Privacy Principle (c) consumers' knowledge and consent are required before their personal data can be collected, used or disclosed. Companies should therefore provide opt-in and opt-out options to ensure compliance.

Further, under Part VIII of the Electronic Transactions Act (Chap 22:05) (although this is not yet in force), any person who sends unsolicited commercial communications through electronic media to consumers in Trinidad and Tobago or knowingly uses an intermediary or telecommunications service provider in Trinidad and Tobago to send, or who has a place of business in Trinidad and Tobago and sends, unsolicited electronic correspondence to consumers, must provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

General Privacy Principle (a) provides that the company will remain responsible for the personal information under its control, even if third parties are engaged. Companies must therefore ensure that third parties handling personal information must comply with the General Privacy Principles.

Before sharing personal information with vendors, companies should inform consumers about the purpose of data collection and obtain knowledge and consent (see General Privacy Principles (b) and (c)).

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies must ensure that personal information remains under their control and responsibility, even when shared with third parties. General Privacy Principle (a) establishes that an organization is responsible for the personal information it manages. Therefore, contracts with vendors should include provisions regarding how the data is processed, stored and protected. To comply with these provisions, contracts with vendors and third parties should include the following, without limitation:

- (a) **purpose limitation:** vendors should only use the information for the specific purpose agreed upon: General Privacy Principle (b);
- (b) **confidentiality and security measures:** vendors should implement safeguards to prevent unauthorized access or misuse of information: General Privacy Principle (g);
- (c) **restrictions on further disclosure:** vendors should not share information with other third parties unless explicitly authorized: General Privacy Principles (d) and (l);
- (d) **compliance with data protection laws:** the agreement should require vendors to comply with local and international data protection standards: General Privacy Principle (l);
- (e) **breach notification obligations:** vendors should be required to notify the company of any data breaches affecting personal information since the company bears the ultimate responsibility for the personal information: General Privacy Principle (a); and
- (f) **data retention and deletion policies:** vendors should delete or return personal data once the contract ends or when it is no longer needed: General Privacy Principle (e).

6.3 **What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?**

Under the Data Protection Act, companies are expected to undertake due diligence measures in their privacy practices to ensure compliance with legal principles, safeguard personal information and mitigate privacy risks.

Due diligence requires companies to implement internal privacy policies, controls and assess the risks associated with processing personal information, especially sensitive personal information. This means that companies should, inter alia, ensure compliance with their data protection protocols and conduct third-party vendor assessments to ensure that there are comparable safeguards in the receiving jurisdiction, where applicable.

Companies should also ensure transparency in their data handling practices. General Privacy Principle (b) requires that the purpose of data collection be clearly identified and General Privacy Principle (i) requires that companies provide individuals with information about their privacy policies and practices. These requirements imply that companies should conduct internal audits and regularly review data protection policies.

The Data Protection Act does not explicitly require privacy impact assessments for private entities although there is such a requirement for public bodies (though not yet in force). However, private entities are still bound by the General Privacy Principles, which require them to ensure that personal information is collected for specific and legitimate reasons, not excessive and retained only as necessary and protected by appropriate safeguards. The General Privacy Principles imply a duty to assess risk. Therefore, while impact assessments are not mandatory under the Data Protection Act for private entities, best practice dictates that companies should conduct internal risk assessments to ensure compliance.

7 **SPECIFIC ADVERTISING PRACTICES**

7.1 **How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?**

As at July 2025, in Trinidad and Tobago there are in force no regulations from a privacy perspective for marketing communications.

However, under Part VIII of the Electronic Transactions Act Chap 22:05 (which, as at July 2025 is not in force) any person who sends unsolicited commercial communications through electronic media to consumers in Trinidad and Tobago or knowingly uses an intermediary or telecommunications service provider in Trinidad and Tobago to send, or who has a place of business in Trinidad and Tobago and sends, unsolicited electronic correspondence to consumers, must provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The Data Protection Act does not address the use of tracking technologies such as cookies, pixels, SDKs or equivalent devices.

Note however, that, under the Computer Misuse Act (Chap 11:17), a person commits an offence if they either knowingly and without authority cause a computer to perform any function for the purpose of securing access to any program or data held in any computer; or, without authority, directly or indirectly commits an act that has the effect of causing the modification of any program or data held in any computer.

Access of any kind by any organization to data held in a computer is unauthorized or done without authority if:

- (a) the organization is not itself entitled to control access of the kind in question to the program or data; and
- (b) the organization does not have the consent of the data subject to access the program or data.

Accordingly, companies should obtain prior authorization to store cookies or equivalent tracking technologies on the data subject's equipment.

7.3 How are loyalty programs and promotions regulated under privacy law?

There is currently no regulation of loyalty programs from a privacy perspective.

7.4 How is social media and influencer marketing regulated under privacy law?

There are currently no privacy laws in Trinidad and Tobago for social media.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

There are no specific regulations with respect to targeted and behavioral advertising, or contextual advertising from a privacy perspective. However, the General Privacy Principles will apply (see question 4.1), especially for targeted advertising which relies on personal information.

However, the Advertising Standard provides that advertisements should not be worded to exploit the vulnerability of any category of consumers.

Further, the Trinidad and Tobago Standard, Requirements for Advertising—Part 2: Advertising to Children (2nd Revision) TTS 94-2:2010 ('the Advertising to Children Standard') regulates advertisements directed at children in Trinidad and Tobago in any medium, regardless of origin.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are currently no specific privacy laws governing digital identity resolution and clean room technologies. However, the General Privacy Principles will apply (see question 4.1).

7.7 How is location-based advertising regulated under privacy law?

There are currently no specific privacy laws governing location-based advertising.

7.8 How are data brokers defined and regulated under privacy law?

There are currently no specific privacy laws governing data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

There are no specific provisions in the Data Protection Act that govern advertising to children or minors. However, such advertising is addressed through industry self-regulation, specifically under the Advertising to Children Standard. However, this standard does not expressly address the use of children's personal information for advertising purposes. Children will therefore be captured as an 'individual' under the Data Protection Act. This means that consent of the individual (parent or guardian in the case of a child), collection for a specific and identified purpose and ensuring the personal information is appropriately safeguarded will apply.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

There are no specific privacy laws governing profiling, the use of artificial intelligence or automated decision making as at July 2025.

7.11 Are there other specific advertising practices that you wish to discuss?

N/A

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The General Principles of the Data Protection Act include that personal information which is requested to be disclosed outside of Trinidad and Tobago must be regulated, and safeguards comparable to those under the Data Protection Act must exist in the jurisdiction receiving the personal information. Moreover, under provisions yet to come into force, where a mandatory code of conduct is developed, it must require, as a minimum, that personal information under the custody or control of an organization must not be disclosed by that organization to any third party without the consent of the individual to whom it relates, except in certain circumstances. Further, companies must inform individuals about who is requesting their data, the purpose of the transfer and the data protection framework in the receiving jurisdiction. Please note that while these provisions are not in force, they represent best practice in Trinidad and Tobago.

Otherwise, there are no special conditions that restrict individuals or organizations from transferring personal data to others within their group who are situated outside of Trinidad and Tobago.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

N/A

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Trinidad and Tobago? Are there minimum standards? Does this differ by sector or size of the entity?

The General Privacy Principles include that personal information is to be protected by such safeguards as are appropriate having regard to the sensitivity of the information. However, there are no specific rules as to what constitutes appropriate safeguards.

The Office of the Information Commissioner is responsible for monitoring the administration of the Data Protection Act to ensure that its purposes are achieved. It may publish guidelines regarding compliance with the Data Protection Act, including guidelines on the development of industry codes of conduct, firm compliance policies, procedures for handling complaints, guidelines dealing with conflict of interest for industry bodies or individuals who mediate or deal with complaint resolution, guidelines dealing with the security of information and information systems, and guidelines for information sharing agreements or data matching agreements.

However, as at July 2025 no officers have been appointed to the Office of the Information Commissioner.

9.2 How are personal data breaches regulated in Trinidad and Tobago? What are the requirements for notification and response?

The Data Protection Act contemplates that, where an individual has a reasonable belief that an organization is not complying with the provisions of the Act or a mandatory code of conduct, they may make a complaint to the Information Commissioner. Upon receiving the complaint, the Information Commissioner may conduct an enquiry and can order the head of the organization to comply with the Act or the mandatory code of conduct. Failure to comply with the order of the Information Commissioner is an offence. However, these provisions of the Data Protection Act are not yet in force.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Once the relevant provisions of the Data Protection Act come into force:

- (a) A person who commits an offence under the Data Protection Act is liable:
 - (i) upon summary conviction, to a fine of not more than TTD 50,000 (approx USD 7,200) or to imprisonment for a term of three years; and
 - (ii) upon conviction on indictment, to a fine of not more than TTD 100,000 (approx USD 14,400) or to imprisonment for a term of not more than five years.
- (b) Where the offences under the Data Protection Act are committed by a body corporate, the body corporate shall be liable:
 - (i) upon summary conviction, to a fine of TTD 250,000 (approx USD 36,200); and
 - (ii) upon conviction on indictment, to a fine of TTD 500,000 (approx USD 72,400).

- (c) Where a corporation contravenes any of the provisions of the Data Protection Act, the court may impose a fine of up to 10% of the annual turnover of the enterprise. The court shall take into account:
- (i) the estimate of the economic cost of the contravention to the consumers, users of the services in question or any other person affected by the contravention;
 - (ii) the estimate of the economic benefit of the contravention to the enterprise;
 - (iii) the time for which the contravention is in effect is continuing;
 - (iv) the number and seriousness of any other contraventions, if any, committed by the corporation; and
 - (v) any other matter the court may consider appropriate in the circumstances.

10.2 Do consumers have a private right of action? What remedies are available to them?

Any disclosure of an individual's personal information may be actionable by that individual bringing a common law action for breach of confidence. The remedies will be in damages for any loss caused by the breach or an injunction to prevent further unauthorized disclosure, if relevant.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Not very active. There are no recent examples of enforcement action for privacy non-compliance in advertising.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Trinidad and Tobago?

There are no cultural considerations which affect privacy law or enforcement. However, once the Data Protection Act is fully proclaimed, it will certainly have a major impact on the culture of privacy in Trinidad and Tobago, particularly in the private sector where there are currently no restrictions on the use of individual's data and it is largely self-regulated.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

N/A

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

No changes.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Once the Data Protection Act is fully proclaimed and enforced, private companies will be required to sensitize themselves to its provisions in order to ensure compliance. The Data Protection Act contemplates harsh penalties for breaches, and companies must re-evaluate their privacy policies and processes to ensure they do not run afoul of the Act.

Companies will need to consider expending sums to invest in software technology to ensure the protection of individuals' personal information under their control or within their custody.

12.3 What do you envision the privacy landscape will look like in five years?

The rapid development in online technology and social media platforms has far outstripped local legislation. These realities will put greater pressure on the Government not only to fully enact the Data Protection Act, in order to ensure the appointment of the Information Commissioner, but also to amend the Act so that it provides more robust protection of individuals' privacy.

TUNISIA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Tunisia.

Privacy in Tunisia is regulated under Organic Law No 2004-63 of July 27, 2004, on the Protection of Personal Data. This law establishes the legal framework for the processing of personal data, ensuring the protection of individuals' privacy rights. It applies to both automated and non-automated data processing carried out by individuals or legal entities. The law mandates transparency, fairness, and respect for human dignity in handling personal data. The National Authority for the Protection of Personal Data ('INPDP') is the regulatory body responsible for overseeing compliance, issuing authorizations, and handling violations.

1.2 What are the primary laws regulating privacy in Tunisia? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The primary law regulating privacy in Tunisia is Organic Law No 2004-63 on the Protection of Personal Data. Additionally, Tunisia has ratified the Council of Europe Convention 108, which reinforces its commitment to international data protection standards. Other relevant laws include:

- (a) the Tunisian Constitution, which guarantees privacy rights;
- (b) the Electronic Communications Code, which regulates electronic data transmission; and
- (c) the Criminal Code, which penalizes unauthorized access to personal data.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation is not explicitly mandated under Tunisian privacy law, but businesses, particularly those in digital advertising, are encouraged to adopt internal compliance measures. The INPDP provides guidelines on best practices, and industry associations may establish voluntary codes of conduct to ensure compliance with privacy obligations.

1.4 How is privacy law enforced in Tunisia? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The INPDP is responsible for enforcing privacy laws in Tunisia. It has the authority to investigate complaints, conduct audits, issue fines, and refer cases for prosecution. Privacy violations can result in administrative penalties and criminal sanctions. Individuals can file complaints with the INPDP, but there is no private right of action to seek damages directly.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Tunisia?

A company is subject to Tunisian privacy law if it processes personal data within Tunisia, regardless of whether it is a local or foreign entity. Both private and public sector entities must comply with data protection requirements, including obtaining authorization for certain processing activities.

2.2 Does privacy law in Tunisia apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, foreign companies operating in Tunisia must comply with Organic Law 2004-63. There are no exemptions based on nationality or legal status. Foreign companies processing data of Tunisian residents may be required to obtain authorization from the INPDP and ensure compliance with data security and consent requirements.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Tunisia?

‘Personal data’ is defined as any information that identifies or can be used to identify a natural person, either directly or indirectly. This includes names, identification numbers, biometric data, and digital identifiers.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

‘Sensitive personal data’ includes racial or ethnic origin, religious beliefs, political opinions, health information, genetic data, biometric data, and criminal records. Processing such data requires explicit consent from the data subject or a legal exemption.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized data that cannot be linked to an individual is not subject to privacy law. However, pseudonymized data that can still be re-identified is considered personal data, and remains regulated under the law.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must obtain consent before processing personal data, ensure data security, provide privacy notices, limit data collection to necessary purposes, and comply with INPDP authorization requirements for certain processing activities. They must also implement safeguards against unauthorized access and maintain records of processing activities.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, companies are classified as either data controllers or data processors. Data controllers determine the purposes and means of processing, while data processors handle data on behalf of controllers and must comply with contractual obligations regarding security and confidentiality.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, processing must be based on consent, legal obligations, contractual necessity, or legitimate interest, provided that it does not infringe on individuals' privacy rights.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Privacy notices must include the purpose of data collection, the legal basis for processing, data retention periods, consumer rights, and mechanisms for redress.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the right to access, correct, and delete their personal data, withdraw consent, and object to data processing, particularly for marketing purposes.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies must obtain explicit opt-in consent for direct marketing via electronic communications and provide clear opt-out mechanisms.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Companies must ensure that third parties processing personal data comply with data protection laws. Contracts with vendors must include provisions on security, confidentiality, and data protection obligations.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Contracts must specify data protection responsibilities, security measures, and compliance requirements, ensuring that third parties handle data lawfully and securely.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must conduct vendor assessments and, for high-risk processing activities, complete data protection impact assessments to identify and mitigate potential risks.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Direct marketing requires prior opt-in consent from individuals. Companies must provide clear opt-out mechanisms, allowing consumers to withdraw their consent at any time. Marketing communications must also include clear identification of the sender and the purpose of the message.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies requires explicit consent from users. Companies must provide transparency regarding the purpose of data collection, allow users to manage their preferences, and ensure compliance with data retention policies.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs must comply with data minimization and purpose limitation principles. Consumers must be informed about how their data will be collected, stored, and used. Data collected for loyalty programs cannot be repurposed without consent.

7.4 How is social media and influencer marketing regulated under privacy law?

Companies using social media and influencer marketing must ensure that personal data collected from users complies with privacy laws. Data collected through engagement tracking, social listening, and behavioral analysis must have a clear legal basis, such as consent or legitimate interest.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising requires user consent when personal data is used for behavioral profiling. Contextual advertising, which does not rely on user tracking but instead serves ads based on webpage content, is generally less regulated.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no explicit regulations on digital identity resolution or clean room technologies in Tunisia. However, general data protection principles apply, requiring organizations to ensure anonymization, encryption, and secure data processing practices.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising requires user consent before collecting geolocation data. Companies must provide users with options to disable location tracking and must ensure data is not retained longer than necessary.

7.8 How are data brokers defined and regulated under privacy law?

Tunisian privacy law does not explicitly define data brokers, but companies engaged in large-scale data collection and resale must obtain authorization from the INPDP. They must also ensure compliance with data processing and transfer requirements.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising targeting minors is subject to stricter regulations, requiring explicit parental consent for data collection. Companies must avoid using behavioral profiling techniques on minors and ensure age-appropriate content in their marketing campaigns.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Profiling and AI-driven decision-making for advertising require transparency, user rights protections, and, in some cases, explicit consent. Companies must inform individuals when automated decision-making is used and provide mechanisms for human review of significant decisions.

7.11 Are there other specific advertising practices that you wish to discuss?

Businesses should be aware of evolving regulations related to biometric advertising, facial recognition, and voice-based marketing, as these areas may face additional scrutiny in the coming years.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Tunisian law requires authorization from the INPDP for personal data transfers to foreign countries. The INPDP evaluates whether the recipient country provides an adequate level of protection before approving the transfer. Specific contractual safeguards, such as standard contractual clauses, may be required for transfers to jurisdictions without recognized data protection standards. Transfers that could threaten national security or public interests are strictly prohibited.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Organizations must obtain written consent from data subjects before transferring personal data. If the data concerns minors, additional authorization from the family judge may be required. Transfers must align with Tunisia's national security policies and international agreements.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Tunisia? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is governed by Organic Law No 2004-63, which requires data controllers and processors to implement appropriate technical and organizational measures to protect personal data against unauthorized access, alteration, and destruction. Security standards may vary by sector, with stricter regulations in areas such as healthcare, banking, and telecommunications.

9.2 How are personal data breaches regulated in Tunisia? What are the requirements for notification and response?

There is no explicit mandatory breach notification requirement under Tunisian law. However, companies handling sensitive data are encouraged to notify the INPDP and affected individuals in cases of significant breaches. Companies must take immediate corrective actions to mitigate any damage caused by a data breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties for non-compliance include fines and imprisonment. Unauthorized data transfers, failure to obtain proper authorizations, and breaches of confidentiality can lead to criminal prosecution, with penalties of up to one year in prison and a fine of 5,000 Tunisian dinars.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers do not have a direct private right of action under Tunisian privacy law. Instead, they must file complaints with the INPDP, which may investigate and impose corrective measures. Courts may provide civil remedies under general liability principles.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The INPDP actively enforces privacy laws, particularly against unauthorized data processing and unlawful data transfers. In 2023, the INPDP referred multiple cases to the public prosecutor for non-compliance, with ongoing legal proceedings against public and private entities for failing to declare their data processing activities.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Tunisia?

Tunisian privacy laws emphasize national security, and government agencies have broad access to personal data. There is also a cultural expectation of strong consumer privacy protections, leading to heightened scrutiny of data-handling practices.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Companies should prepare for potential updates aligning Tunisian law with GDPR standards, increased enforcement actions against non-compliant businesses, and stricter regulations on biometric data and artificial intelligence-driven profiling.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Organizations should proactively assess their data processing activities, seek necessary authorizations from the INPDP, and ensure compliance with security and data retention requirements to avoid regulatory penalties.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The increased focus on data localization and stricter enforcement by the INPDP have been major developments since 2022. Global trends and Tunisia's commitment to aligning with international data protection standards have influenced these changes.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Challenges include navigating complex data transfer regulations, obtaining INPDP approvals, and implementing robust security measures to mitigate regulatory risks.

12.3 What do you envision the privacy landscape will look like in five years?

Tunisia is expected to move toward a more GDPR-aligned framework, with greater emphasis on consumer rights, data portability, and stricter compliance requirements for companies handling personal data.

 TURKEY 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Turkey.

The Turkish Constitution recognizes the privacy of an individual as a human right. However, the main legislation governing privacy in Turkey is the Data Protection Law ('DPL'), which came into force on April 7, 2016. The DPL is modelled on the former EU Data Protection Directive (95/46) but it is not a replica; there are certain differences, some of which are important. However, in general, the DPL is quite similar to the EU Directive, embracing also some concepts from the GDPR.

1.2 What are the primary laws regulating privacy in Turkey? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The main legislation governing privacy in Turkey is the DPL. The Turkish Penal Code also includes some provisions for illegal transfer or collection of personal data.

The Data Protection Board ('Board'), which is the executive body of the Data Protection Authority ('DPA'), issues secondary legislation which details the obligations set out under the DPL.

There are also sector-specific provisions in the laws and regulations in the electronic communication, finance, insurance and capital markets sectors. There is no provision under Turkish law that focuses on the privacy aspects of advertising. The advertising aspects are subject to the general provisions of the DPL.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The DPL imposes strict statutory obligations on data controllers, ensuring that privacy compliance is governed by legally binding rules rather than voluntary industry standards.

While the DPL does not explicitly promote self-regulation, industry bodies and associations may develop best practices for privacy-compliant advertising. However, these must align with the DPL's legal framework and cannot weaken statutory requirements.

1.4 How is privacy law enforced in Turkey? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

- (a) The DPA is the regulator that enforces the DPL. The enforcement decisions are made by the Board, which is the executive body of the DPA. In situations where a complaint is involved, or where the Board becomes aware of non-compliance with the DPL, the Board can conduct an investigation into the matter to determine whether or not there is any such non-compliance. In case of non-compliance, the Board can:
 - (i) request that the data controller comply with DPL; and/or
 - (ii) impose administrative fines on data controllers.
 In addition, non-compliance with the provisions related to personal data can result in criminal sanctions.

Since its establishment in January 2017, the Board has followed up and investigated violations of the DPL and its secondary legislation, and has rendered many decisions where it has imposed administrative fines.

- (b) The Turkish Penal Code regulates some crimes related to privacy.
- (c) Alternatively, if the data subject suffers material or moral damage due to the violation of their rights regarding personal data, they have the opportunity to claim compensation before the civil courts. In this context, the rights of the data subjects are regulated by the Turkish Civil Code in terms of personal rights and the Turkish Code of Obligations in terms of delictum and compensation law.
- (d) Finally, some sectors have their own regulatory authorities such as the Advertisement Board, the Banking Regulation and Supervision Board, the Information Technologies and Communication Board, and these regulatory authorities can also make regulations on the personal data protection and privacy issues in terms of the relevant sectors.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Turkey?

Regardless of the legal structure, nationality or the domicile of the data controller, all natural or legal persons who process the personal data of natural persons residing in Turkey, wholly or partly by automatic means, or by non-automatic means as a data controller provided that it is a part of a data registration system, are subject to the DPL.

2.2 Does privacy law in Turkey apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

There is no specific territoriality provision under the DPL. However, as the stated purpose of the DPL is to protect the privacy rights of individuals, it can be extrapolated that the DPL is applicable to data controllers both inside and outside Turkey, as this is necessary in order for the DPL to be able to protect the privacy rights of individuals in Turkey. Otherwise, the purpose of the DPL cannot be achieved. It has further been indicated by the DPA that any data controller targeting personal data in Turkey is subject to the DPL.

Data controllers located abroad are under an obligation to be registered with VERBIS (the data controllers' registry in Turkey) and to appoint a representative in Turkey, which can be a legal entity or a Turkish citizen residing in Turkey. Other than this, data controllers located outside Turkey are under the same obligations as data controllers located inside Turkey.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Turkey?

Under the DPL, 'personal data' is defined as 'any information relating to an identified or identifiable natural person.' In this framework, all kinds of information from a person's name, surname and ID number to biometric and genetic data are considered as personal data.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, biometrics and genetics are special categories of personal data ('sensitive personal data') as defined under the DPL.

Important amendments have been enacted in the DPL recently. Before such amendments, the processing of sensitive personal data under the DPL was primarily conditional on obtaining the explicit consent of the data subject; and processing such data without explicit consent was almost legally impossible.

With the enactment of the amendments, which aim to address the bottleneck experienced in practice and align with GDPR standards, the conditions for processing sensitive personal data have been expanded, and the distinction between personal data related to health or sexual life and other categories of sensitive personal data has been removed.

Accordingly, all categories sensitive personal data (including health data and personal data related to sexual life) may only be processed if one of the following conditions is met:

- (a) the explicit consent of the data subject is obtained;
- (b) it is expressly stipulated by laws;
- (c) it is necessary for the protection of the life or physical integrity of the data subject or another person who is unable to give consent due to physical impossibility, or whose consent is not legally valid;
- (d) it is relevant to personal data publicized by data subject and is in accordance with the intention of data subject of making it public;
- (e) it is necessary for the establishment, exercise, or protection of a right;
- (f) when processing is compulsory by persons under the secrecy obligation or competent authorities or institutions for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning, management, and financing of health services;
- (g) it is necessary for fulfilment of legal obligations relating to employment, occupational health and safety, social security, social services, and social benefits; or
- (h) where processing is carried out by foundations, associations, and other non-profit organizations or formations established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with the relevant legislation to which these organizations are subject and aligned with their stated purposes, processing is limited to their field of activity, and data is not disclosed to third parties; processing pertains to their current or former members, affiliates or individuals who are in regular contact with these organizations and formations.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Anonymized data is regulated under the DPL, but pseudonymized or de-identified data are not. Therefore pseudonymized and de-identified data are still held as personal data and privacy laws apply to them.

Anonymization of personal data is required if the data controller has no reason left to process personal data further. Anonymization or destruction or erasure of personal data is the required method when the personal data is no longer needed for processing. There is a regulation prepared detailing destruction, anonymization and erasure of personal data dated 28.10.2017.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

- (a) Personal data must be processed on the basis of one of the legal grounds set out in the DPL (see question 4.3) and in accordance with the principles set forth under the DPL. The principles to be complied with when processing personal data are:
 - (i) being in conformity with the law and good faith;
 - (ii) being accurate and, if necessary, up to date;
 - (iii) being processed for specified, explicit, and legitimate purposes;
 - (iv) being relevant, limited and proportionate to the purposes for which the data is processed; and
 - (v) being stored only for the time designated by relevant legislation or necessitated by the purpose for which data are collected.
- (b) Another important obligation is the duty to inform data subjects. Before processing personal data, data controllers must inform the data subjects of the following issues with a privacy notice:
 - (i) the identity of the data controller and its representative (if the data controller is located abroad);
 - (ii) the purposes for which personal data will be processed;
 - (iii) the persons to whom personal data might be transferred and the purposes for the transfer;
 - (iv) the method and legal basis of collection of data; and
 - (v) the rights of data subjects set forth under the DPL.
- (c) Data controllers located abroad must appoint a representative, who must be a Turkish citizen or a legal entity located in Turkey. Data controllers located inside Turkey must appoint Turkish citizens as their contact persons. The representatives/contact persons are designed to be points of contact between data controllers and the DPA and/or the data subjects.
- (d) Data controllers must register with the Data Controllers' Registry, which is an online platform called VERBIS. In order to register with VERBIS, a simplified personal data inventory must be prepared and submitted to the online VERBIS system. The simplified personal data inventory should include the following:
 - (i) categories of personal data processed by the data controller;
 - (ii) the purposes of processing of each personal data category;
 - (iii) data subject groups;
 - (iv) groups of recipients of personal data;
 - (v) whether or not the relevant personal data category is transferred abroad;
 - (vi) measures taken for the security of personal data; and
 - (vii) the maximum period of retention.

- (e) Regarding data security, the data controller should take all necessary technical and organizational measures to provide an appropriate level of security in order to prevent unlawful processing of personal data, prevent unlawful access to personal data, and safeguard personal data.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The DPL has made a binary distinction in this regard: data controller and data processor:

- (a) The **data controller** is defined as the natural or legal person who determines the purposes and means of processing personal data. Data controllers bear the primary legal responsibility for ensuring compliance with the DPL.

Key obligations of data controllers under the DPL include:

- (i) ensuring a lawful basis for data processing,
- (ii) lawful transfer of personal data (cross border transfers),
- (iii) providing clear privacy notices to data subjects,
- (iv) registering with VERBIS, the Turkish Data Controllers' Registry, if applicable,
- (v) implementing technical and administrative security measures to protect data from unauthorized access, loss, or breaches,
- (vi) ensuring data subject rights such as access, correction, and deletion, and
- (vii) supervising third-party processors to maintain compliance with the DPL regulations.

- (b) The **data processor** is defined as the natural or legal person who processes personal data on behalf of the data controller. Unlike controllers, processors do not determine the purpose or means of data processing but act solely under the controller's instructions.

Key obligations of data processors under the DPL include:

- (i) processing personal data only as instructed by the controller and for the specified purpose,
- (ii) implementing security measures to ensure confidentiality, integrity, and availability of personal data, and
- (iii) assisting controllers in fulfilling data subject rights upon request.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

The DPL allows for the processing of personal data without consent under specific legal grounds, including:

- (a) if the processing is explicitly mandated by law;
- (b) if the data subject is unable to provide consent due to physical impossibility or lacks legal capacity, and processing is necessary to protect their or another person's life or bodily integrity;
- (c) if processing is necessary for the establishment or execution of a contract in which the data subject is a party;
- (d) if processing is necessary for the data controller to comply with its legal obligations;
- (e) if the data has been made public by the data subject;
- (f) if processing is necessary for the exercise or protection of a legal right; or
- (g) if processing is necessary for the legitimate interests of the data controller, provided it does not violate the fundamental rights and freedoms of the data subject.

These legal bases ensure that personal data processing remains lawful even in the absence of explicit consent, provided that at least one of these conditions is met.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

In the privacy notices they send to their customers, companies need to include information on:

- (a) identity of the data controller,
- (b) the purpose of data processing,
- (c) with whom the personal data will be shared and the purpose of sharing,
- (d) method of personal data collecting and the legal basis,
- (e) data subjects' rights provided under the DPL (see question 5.2).

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Under the DPL, everyone, by applying to the data controller, has the right to:

- (a) learn whether or not their personal data has been processed;
- (b) request information as to processing, if their data have been processed;
- (c) learn the purpose of processing the personal data and whether data is being used in accordance with this purpose;
- (d) know any third parties in Turkey or abroad to which their personal data has been transferred;
- (e) request rectification in cases where their personal data has been processed incompletely or inaccurately;
- (f) request deletion or destruction of their personal data within the framework of the conditions set out in the DPL;
- (g) request notification of the actions taken under (e) and (f) above to third parties to which personal data has been transferred;
- (h) object to the occurrence of any outcome that is to their detriment resulting from analysis of personal data exclusively through automated systems; and
- (i) request compensation in cases where the data subject incurs damage due to the unlawful processing of their personal data.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Electronic marketing communications is regulated under the Law on Regulation of Electronic Commerce. Under this law, electronic marketing communication messages (such as emails, SMS, etc) can be sent to consumers only with their permission; opt-in consent is required for such communication. The relevant electronic message should also include an opt-out mechanism so that the consumer can easily choose not to receive any further electronic marketing messages.

If the intended recipient is not a consumer but a merchant, there is no need for an opt-in consent for electronic marketing communication. However, the message should still include an opt-out mechanism.

Apart from the activity of sending messages, all other processing activities for marketing communication are regulated by the general provisions of the DPL from a privacy perspective.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The DPL also regulates the transfer of personal data. Personal data may be transferred without explicit consent in the presence of one of the grounds for processing personal data set out in question 4.3. In particular, advertising agencies may use the execution of contract legal base for personal data processing or consent can be also considered to be obtained from third parties (data subjects). However, adequate measures must be taken during these transfers. Privacy notices must be provided specifically in case of use of vendors. If an advertising agency is acting as a representative, the identity of the data controller must be provided properly.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies have duties to:

- (a) fulfil audit requirements;
- (b) ensure that relevant measures (administrative and technical) are taken, and personal data will not be used/processed other than the purpose of the contract; and
- (c) report data breach incidents in a timely fashion,

and must ensure that their contractual obligations comply with the DPL when transferring personal data to or from vendors or third parties. Clearly defining the roles of the parties involved (as data controllers or data processors) is crucial, as obligations differ based on these roles.

The DPL provides that data controllers and data processors are jointly and severally responsible for taking all necessary technical and administrative security measures. This obligation aims to make data controllers pay attention to whom they choose to act as their data processors. If they do not choose a data processor capable of taking the necessary measures in case of a breach, the data controller will also be liable for the failure of the data processor. Of course, the data controller may put a provision in the agreement to have recourse to the data processor in case the data controller is obliged to pay compensation or an administrative fine. However, the main responsible party vis-à-vis the DPA will always be the data controller.

The DPL does not include a provision that explicitly requires data controllers to enter into an agreement with their data processors. However, the DPA has issued guidelines where it states that there should be such an agreement between the data controller and the data processor as an administrative security measure. In addition, the Board has published sample undertakings to be executed between data controllers and data processors (governing cross border transfers). Whilst, these undertakings are not a mandatory general form to be used in all transactions between data controllers and data processors, but rather for cases where a data transfer will be made outside Turkey, they give an idea as to what the DPA considers important in an agreement between a data controller and a data processor. Based on these samples, it is evident that the most important issue for the DPA is security; it wants data processors to take all necessary security measures, and for this issue to be included in agreements between data controllers and data processors

For cross-border data transfers, see question 8.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies are expected to conduct comprehensive due diligence to ensure compliance with DPL and other relevant legislation. This includes:

- (a) ensuring that technical and administrative safeguards are properly implemented;
- (b) confirming that cross-border data transfers have appropriate safeguards in place, such as SCCs;
- (c) validating that explicit consent is obtained where necessary and meets legal requirements;
- (d) ensuring that other data transfers by the third party comply with legal and contractual obligations; and
- (e) ensuring that audit right can be duly exercised.

Although the DPL does not explicitly mandate data protection impact assessments, conducting data protection impact assessments is strongly recommended—especially for advertising practices that involve profiling, tracking, large-scale data processing, or automated decision-making or processing sensitive data. Impact assessments help companies identify and mitigate potential privacy risks, ensuring compliance with transparency, data minimization, and accountability principles.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

- (a) Direct marketing activities, including emails, text messages, and push notifications, are primarily regulated under the Law on the Regulation of Electronic Commerce. The Law on the Regulation of Electronic Commerce and its secondary regulation, the Regulation on Commercial Communication and Commercial Electronic Messages, require companies to obtain opt-in consent before sending any commercial messages via electronic means. Consent must be recorded and managed through the Commercial Electronic Message Management System, a centralized platform where consumers can manage their preferences.
- (b) Under the DPL, individuals have the right to request access to their data, request correction or deletion, and object to its processing for marketing purposes. Businesses must provide an easy mechanism for users to exercise these rights (opt-out mechanism).
- (c) Lastly, as a general responsibility, under the DPL, businesses conducting direct marketing must implement technical and administrative measures to prevent unauthorized access, loss, or unlawful sharing of personal data.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Under Turkish Law, there is no provision specific to the use of tracking technologies. However, using tracking technologies should be considered processing of personal data under the general provisions of the DPL. Under these provisions, based on the level of tracking, the activity would most likely require the consent of the data subject.

Notwithstanding the above, the DPA has published guidelines on the application of cookies. These include a definition of a ‘cookie’ and classify cookies depending on their function, duration, etc. The guidelines further clarify that cookie practices that involve processing of personal data shall be subject to the DPL. In other words, if the use of a particular cookie relies on legal grounds other than explicit

consent, no consent shall be required. If not, consent of the website visitor should be obtained before personal data is collected and processed via such cookies. The guidelines also give examples of good and bad cookie practices.

7.3 How are loyalty programs and promotions regulated under privacy law?

These issues are regulated under the general provisions of the DPL. There is a decision of the Board on a loyalty program of a supermarket. In that decision, the processing of the personal data of participants of a loyalty program was carried out on the basis of the explicit consent of the participants. The Board reviewed the validity of the explicit consents and stated that they were valid because the supermarket did not force its customers to participate in the program and that it continued to sell goods to non-participants, albeit without certain benefits granted only to participants. The Board stated that the existence of choice is an indicator that participants willingly gave their consent for processing.

On June 16, 2022, the DPA released draft Guidelines on the Examination of Loyalty Programs under the Personal Data Protection Legislation, which outlines best practices for handling personal data within these programs. The draft Guidelines define loyalty programs as strategies involving personal data processing for rewards and personalized marketing. Data processing must have a valid legal basis, with explicit consent required for profiling and additional marketing. Consent cannot be a condition for program participation, and incentives must not disadvantage non-participants. Businesses need explicit consent for marketing communications and must provide clear privacy notices. For joint programs, consent is required for advertising-related data sharing.

7.4 How is social media and influencer marketing regulated under privacy law?

From a privacy perspective, social media is regulated under the general provisions and rules of the DPL. There are no specific rules or provision for social media and influencers. In addition, the Law on the Prevention on Crimes committed through the Internet provides that an individual can request the removal of content if such content violates their privacy.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Under Turkish law, there is no provision specific to targeted advertising and contextual advertising. However, the general rules and principles under the DPL are applicable to the targeted advertising. Since targeted advertising requires personal data processing, it is necessary to obtain the explicit consent of the data subject under the DPL, and the other provisions of the DPL will also be implemented. However, the DPL is not applicable to contextual advertising, as there is no personal data processing.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not explicitly regulated under the DPL. However, their use must comply with general data protection rules and principles.

When companies use digital identity resolution to link personal data across multiple sources, they must ensure they have the explicit consent of the data subject or the other valid legal basis for processing. If profiling or personalized marketing occurs, explicit consent is also importantly required. Additionally, in those circumstances, the data subject has the right to object to the occurrence of any outcome that is to their detriment resulting from analysis of their personal data exclusively through automated systems.

Clean room technologies allow companies to match and analyze data while maintaining privacy protections. If data is fully anonymized, it falls outside the scope of the DPL. However, the data remains subject to DPL rules if it can still be linked to an individual. Companies must take security measures to ensure that the data remains protected and that unauthorized re-identification does not occur. Further data subjects must be duly informed of data processing activities and purposes clearly so that if their consent is needed, they are well informed in advance.

Additionally, the use of clean room technologies may also raise concerns under competition law. If companies engage in data sharing through clean rooms in a way that restricts competition or creates barriers to market entry, competition authorities may scrutinize these practices. Therefore, businesses should ensure that data collaboration does not lead to anti-competitive behavior. In this context, the European Commission imposed a fine of approximately €797 million on Meta in November 2024 for abusing its dominant position in online advertising markets, which highlights the regulatory focus on data-driven competition concerns. Similarly, in Turkey, the Competition Authority launched an investigation into Meta in November 2023 regarding its integration of Instagram and Threads without user consent, leading to a temporary injunction and a fine of approximately TRY 335 million (approx USD 8.5 million).

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not explicitly regulated under the DPL. However, the principles outlined in question 7.1. also apply in this context. Accordingly, obtaining explicit consent from individuals, and fulfilling transparency obligations are necessary. Nevertheless, real-time location-based advertising is critical. Although there are no explicit provisions prohibiting it, such practices may exceed the limits set by general principles, particularly in terms of being relevant, limited, and proportionate to the purposes for which the data is processed.

7.8 How are data brokers defined and regulated under privacy law?

No, under Turkish Law, there are no specific rules governing data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

Under Turkish Law, there is no provision specific to the processing of children's and minors' personal data. The general rule is that parental consent is required for processing personal data of persons under 18. However, the recent statements made by Turkish senior officials and ministers indicate that regulations similar to the GDPR will be adopted in the near future. Further it is also important to provide adequate privacy notices to children and minors when processing their personal data. Parental control mechanisms must be in place as well.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

In addition to the general regulations and principles on the processing of personal data and the rights of data subjects, the DPL sets out a special rule on automated decision-making systems. Within this framework, the data subject has the right to object to the occurrence of any outcome that is to their detriment resulting from analysis of their personal data exclusively through automated systems. Recently the DPL issued guidelines on the use of AI from a data privacy perspective. The rules detailed in the guidelines apply to advertising as well.

7.11 Are there other specific advertising practices that you wish to discuss?

From the privacy perspective, there are no additional specific advertising practices beyond those already covered.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

There have been major amendments made to the DPL regarding the transfer of personal data outside Turkey. Prior to the amendments, personal data could, in the main, be transferred abroad only with the explicit consent of the data subject, as the other legal grounds specified in the legislation were either not available or not applicable. In this context, the amendments introduced a three-stage assessment system for cross-border data transfer. Now personal data can be transferred abroad if one of the legal processing grounds specified in the Law is present and if the Board issues an adequacy decision. In cases where no adequacy decision is available, data can be transferred abroad if the parties involved provide one of the appropriate safeguards listed in the Law, namely:

- (a) **Binding corporate rules:** Data controllers that are part of a multinational group of organizations may prepare binding corporate rules regarding inter-company data transfers in accordance with the guidelines on binding corporate rules to be published by the DPA and submit them to the Board for approval. Within the framework of the binding corporate rules approved by the Board, data may be transferred to the parent company and its affiliates located abroad;
- (b) **Undertaking:** The data exporter and importer may prepare a written undertaking providing adequate protection for personal data in accordance with the Law and the secondary regulations of the DPA, and apply for the permission of the Board. In the existence of such permission, data may be transferred to the parties of such undertaking(s).
- (c) **Standard contracts:** In the absence of the aforementioned approvals and permissions, it is also possible to sign standard contracts that will be announced by the Board. Such contracts must be executed without making any amendments, and the standard contracts to be executed must be notified to the Board (with the documents showing the signatures, authorities of signatories to sign such contracts, and notarized Turkish translations of such documents) within five business days from the date of execution. The draft standard contracts have been published by the Board and the final versions are expected to be announced soon. Whilst standard contracts cannot be used until the final versions are published, as a preliminary preparation when waiting for the final versions, it is extremely important for data controllers who wish to continue their transfers abroad by providing this assurance to map their transfers abroad. These contracts should include the parties, the activities of the data exporter and data importer regarding personal data to be transferred, the relevant groups of data subjects, the scope of the transferred personal data, the legal grounds for the transfers, the frequency of the transfers, the nature of the processing activity, the purposes of the transfer and subsequent processing activities, the retention periods, the recipient groups and the data transferor's Data Controllers' Registry information (if available).

At least one of the above safeguards should also be provided for any subsequent cross-border transfers of personal data.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Standard contracts (see question 8.1), considered one of the most significant changes introduced by the amendments in the DPL, resemble the standard contracts under the GDPR framework. The published standard contracts (templates) require extensive preparation by both the data recipient and the data transferring party and necessitate the provision of information on the following matters:

- (a) the activities of both the data transferring party and the data recipient regarding the transferred personal data;
- (b) the data subject groups whose personal data is being transferred;
- (c) the categories of transferred personal data and, if applicable, the categories of transferred special category personal data;
- (d) the legal basis for the transfer;
- (e) the frequency of the transfers;
- (f) the nature of the data processing activity;
- (g) the purposes of data transfer and subsequent processing activities;
- (h) the retention period of personal data;
- (i) the recipients or recipient groups;
- (j) the data controller's registration details in the Data Controllers' Registry Information System ('VERBIS');
- (k) in cases of transfer to data processors or sub-processors, the subject, nature, and duration of the processing activity;
- (l) the technical and administrative measures implemented, and, if special categories of personal data are transferred, the additional technical and administrative measures taken specifically for such transfers; and
- (m) if applicable, the list of sub-processors.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Turkey? Are there minimum standards? Does this differ by sector or size of the entity?

Data security in Turkey is primarily governed by the DPL, which imposes strict obligations on data controllers and processors to ensure the confidentiality, integrity, and availability of personal data.

The DPL mandates that data controllers and processors take technical and administrative measures to prevent unlawful processing, unauthorized access, and data breaches. Whilst the DPL does not prescribe specific technical standards, the Board's Guidelines on Security of the Personal Data outlines essential technical and administrative measures that data controllers must implement to ensure compliance with data protection regulations:

- (a) The Guidelines highlight the following key technical safeguards to protect personal data:
 - (i) **authorization matrix:** defining and restricting access levels for users based on necessity;
 - (ii) **access control:** ensuring that only authorized personnel can access sensitive data;
 - (iii) **access logging:** keeping records of who accesses personal data and when;

- (iv) **user account management:** monitoring and securing user accounts to prevent unauthorized access
 - (v) **network security:** implementing firewalls, VPNs, and secure configurations to protect data traffic;
 - (vi) **application security:** ensuring that software and applications handling personal data have necessary security measures;
 - (vii) **encryption:** encrypting sensitive data to prevent unauthorized disclosure;
 - (viii) **penetration testing:** conducting security tests to detect vulnerabilities in IT systems;
 - (ix) **intrusion detection and prevention systems:** monitoring and blocking unauthorized access attempts;
 - (x) **log records:** keeping detailed logs for security audits and compliance tracking;
 - (xi) **data masking:** obscuring sensitive data to minimize exposure risks;
 - (xii) **data loss prevention ('DLP') software:** preventing unauthorized data transfers or leaks;
 - (xiii) **backup procedures:** regularly backing up personal data to prevent loss due to cyber incidents;
 - (xiv) **firewalls and updated anti-virus systems:** protecting IT infrastructure from cyber threats;
 - (xv) **deletion, destruction, or anonymization:** implementing proper procedures to erase data securely when no longer needed.; and
 - (xvi) **key management:** securing encryption keys to maintain data confidentiality.
- (b) The Guidelines also emphasize administrative safeguards to ensure organizational compliance, including:
- (i) **preparation of a personal data processing inventory:** documenting how and why personal data is processed;
 - (ii) **corporate policies:** establishing security policies such as access management, data retention, and disposal policies;
 - (iii) **contracts:** ensuring agreements between data controllers and processors include data protection obligations;
 - (iv) **confidentiality commitments:** requiring employees and third parties to sign confidentiality agreements;
 - (v) **internal periodic and/or random audits:** conducting regular checks to ensure compliance;
 - (vi) **risk assessments:** identifying and mitigating potential security threats;
 - (vii) **employment contracts and disciplinary regulations:** integrating DPL compliance clauses into employment policies;
 - (viii) **corporate communication policies:** establishing crisis management, breach notification, and reputation management procedures;
 - (ix) **training and awareness programs:** educating employees on personal data protection and information security; and
 - (x) **notification to VERBIS:** Registering with the Data Controllers' Registry System and ensuring compliance.

Under normal circumstances, these minimum standards do not differ by sector or size of the entities but there are some additional measures in certain industries such as financial, telecommunications, healthcare, etc.

9.2 **How are personal data breaches regulated in Turkey? What are the requirements for notification and response?**

Under the DPL, data controllers are legally required to implement technical and administrative measures to prevent unlawful access, unauthorized processing, and potential data breaches. In the event of a breach, data controllers must act swiftly and follow the procedures established by the Board, by which, if personal data is unlawfully accessed or compromised, the data controller must notify both the DPA and the affected individuals without undue delay and no later than 72 hours after becoming aware of the incident. If a delay is unavoidable, the controller must provide justification. Affected individuals must be informed directly if their contact details are available; otherwise, the notification must be made through appropriate public channels, such as an announcement on the company's website.

Additionally, data processors are required to report any breaches to the data controller immediately.

If the breach occurs within a foreign-based organization but affects individuals in Turkey, the controller must still notify the DPA under the same principles.

The notification must be submitted using the personal data breach notification form, and, if all necessary details are not immediately available, further information must be provided progressively. Data controllers must maintain detailed records of all data breaches, their impact, and the actions taken to mitigate risks. These records must be made available for review by the DPA upon request.

To enhance preparedness, data controllers should establish a comprehensive breach response plan, which includes incident detection, immediate containment measures, impact assessment, regulatory notifications, and post-breach remediation. Regular testing and updates of this plan are essential to ensure an effective and swift response to any future data breaches.

10 **ENFORCEMENT AND PENALTIES**

10.1 **What penalties exist for non-compliance with privacy law?**

(a) **Administrative fines:**

- (i) if the data controller does not provide sufficient information to the data subject as to the nature and purpose of processing as required by the DPL, it will be subject to an administrative fine between TRY 47,303 and TRY 946,308 (approx USD 1,289–25,794);
- (ii) if the data controller or data processor does not take the necessary safety measures as required by the DPL, it will be subject to an administrative fine between TRY 141,934 and TRY 9,463,213 (approx USD 3,868–257,946);
- (iii) if the data controller or the data processor does not comply with the decisions of the Board, it will be subject to an administrative fine between TRY 236,557 and TRY 9,463,213 (approx USD 6,448–257,946); and
- (iv) if the data controller does not register itself with the Data Controllers' Registry, it will be subject to an administrative fine between TRY 189,245 and TRY 9,463,213 (approx USD 5,158–257,946).

(b) **Criminal sanctions:**

- (i) for unlawfully recording the personal data of another, imprisonment of 1–3 years;
- (ii) for unlawfully transferring/acquiring another person's personal data to/from another person, imprisonment of 2–4 years,
- (iii) for not anonymizing, deleting or destroying personal data after the legally permitted period, imprisonment of 1–2 years.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under the DPL, data subjects have the right to request compensation if they suffer damage due to processing of their personal data in violation of the DPL. A claim for such compensation is not made to the Board but to the civil courts. Data subjects can also make a complaint to the Board in relation to the violating activity, in which case the remedy would be for the Board to order the cessation of such activity.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The DPA has been active in enforcing privacy regulations, particularly in cases involving advertising and marketing. Enforcement actions often focus on improper data processing, lack of explicit consent, and failure to fulfill disclosure obligations or to take all necessary technical and administrative measures.

The Board (in decision 2022/1072) has ruled that processing a data subject's email address for advertising purposes without explicit consent constitutes a violation of the DPL. The decision determined that the data controller was responsible for an unauthorized email sent by a former employee, leading to the imposition of an administrative fine of TRY 50,000. Additionally, the unlawfully processed personal data was ordered to be deleted, and the deletion process was to be documented and reported to the Board.

As another recent example, the Board (in decision 2024/1385) evaluated a data breach notification submitted by an e-commerce platform. As a result of a data breach, unauthorized individuals accessed 673 sellers and 7,202 customers' personal data. The Board determined that the data controller failed to implement necessary security measures, such as two-factor authentication and real-time anomaly detection, before the breach. Consequently, the Board imposed an administrative fine of TRY 3,250,000.

The Board has, so far, primarily focused on handling complaints and investigating data breaches, rather than proactively conducting *ex officio* investigations (apart from acting against globally-known data controllers), despite having the authority to do so. Consequently, it has positioned itself as an enforcement authority rather than a guiding authority. However, this approach is expected to evolve in the near future, with the Board taking a more proactive stance. In this context, sector-based investigations are likely to be initiated, signaling a shift towards a more structured and systematic regulatory approach. This change aligns with Turkey's increasing efforts to harmonize with EU data protection standards, indicating that enforcement practices may continue to develop in a more strategic and preventative direction.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Turkey?

N/A

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

One of the hot topics in Turkey’s evolving privacy landscape is cross-border data transfers and standard contracts (see question 8). The recent amendments to the DPL introduced a new transfer mechanism, similar to that in the GDPR, allowing companies to rely on standard contracts instead of explicit consent. Businesses must now navigate the implementation of standard contracts, ensure compliance with notification requirements, and update their privacy frameworks accordingly. As companies adapt to these changes, cross-border data transfers and standard contracts compliance remain key areas to monitor.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Turkish data protection framework is increasingly aligning with EU practices, and this trend is expected to continue. Future regulations may further address areas such as automated decision-making and the processing of children’s personal data, reinforcing Turkey’s EU harmonization efforts. Given this trajectory, companies should anticipate further regulatory developments and ensure that their privacy policies, data governance strategies, and compliance frameworks are structured in accordance with EU standards to remain adaptable and future-proof.

More AI related regulations are expected in the near future. The DPA has recently issued guidelines on the use of AI from privacy perspective.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since the last publication in 2022, Turkey’s privacy landscape has undergone significant changes with the amendments introduced into the DPL which introduced new regulations on sensitive personal data processing (see question 3.2), cross-border data transfers (see questions 8.1 and 8.2), administrative sanctions and legal remedies.

Before the amendments, processing sensitive personal data relied almost exclusively on explicit consent, creating legal and practical challenges when consent was impractical. The rigid framework also failed to address distinctions between different types of sensitive data, prompting a need for broader legal bases.

Likewise, cross-border transfers were restricted due to the absence of an adequacy decisions and the burdensome approval process for safeguards, such as undertakings, which led to significant delays. As a result, explicit consent remained the primary option, causing disruptions when withdrawn. By expanding legal bases, introducing alternative transfer mechanisms, these reforms have enhanced legal certainty and support Turkey’s alignment with EU data protection standards.

The amendments also clarify the judicial review process for administrative fines imposed by the Board. Moving forward, such fines imposed can be directly challenged before administrative courts, providing clearer legal recourse for data controllers and processors.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Currently, one of the most pressing issues for companies is adapting to the new standard contracts regime introduced under the recent amendments to the DPL. Unlike the GDPR framework, the Turkish standard contracts must be submitted to the DPA within five business days, creating an additional compliance burden. Companies must ensure that standard contracts are drafted, negotiated, and signed within a short time frame to avoid potential administrative sanctions.

Another key challenge is the preparation and updating of privacy notices. With the evolving regulatory landscape, companies need to revise their privacy policies to align with the latest legal requirements and ensure that data subjects are properly informed about data processing activities.

Additionally, the tight three-month transition period given for compliance with these new rules has posed a significant challenge.

Looking ahead, while no major legislative overhauls are expected in the near term, incremental regulatory updates in line with EU harmonization efforts could introduce further obligations. Therefore, companies should stay vigilant and closely monitor regulatory developments to maintain compliance. We may expect further regulatory actions for use of AI.

12.3 What do you envision the privacy landscape will look like in five years?

Looking ahead, no major amendments to the DPL are expected, except for AI, in the near future. However, minor adjustments may be introduced as part of EU harmonization efforts, aiming to further align Turkish data protection regulations with the GDPR, other EU legislation, and practices.

UGANDA

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Uganda.

Uganda regulates privacy through the Constitution of the Republic of Uganda, the Data Protection and Privacy Act Cap 97 ('DPPA') and the Data Protection and Privacy Regulations 2021 ('DPP Regulations'). The Constitution recognizes the right to privacy, and the DPPA further outlines the protection of personal data. The DPPA mandates that personal data processing must be fair, lawful, and transparent, and it establishes the Personal Data Protection Office ('PDPO') within the National Information Technology Authority (NITA-U) to oversee its implementation. The PDPO is an independent statutory authority tasked to oversee the lawful collection, control, and processing of personal data. NITA-U is responsible for promoting and regulating information technology, including data protection and privacy.

1.2 What are the primary laws regulating privacy in Uganda? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The general framework of statutes that cater to the protection of the right to privacy in Uganda comprises:

- (a) Constitution of the Republic of Uganda;
- (b) DPPA;
- (c) DPP Regulations ;
- (d) Communications Act Cap 103;
- (e) Access to Information Act Cap 95;
- (f) Regulation of Interception of Communications Act Cap 101; and
- (g) Computer Misuse Act Cap 95.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

The DPPA sets out formal obligations on consent, data collection, and processing. It does not comprehensively regulate advertising-specific practices like behavioral targeting, influencer disclosures, or tracking technologies.

In addition, the Uganda Communications Act mandates the Uganda Communications Commission ('UCC') to set standards, monitor, and enforce compliance relating to content in Uganda. In 2019, the UCC published Advertising Standards which lay down rules on communication of advertisements on all platforms regulated by the Commission under the Act; such as radio, television, and online media. These Advertising Standards serve to ensure that:

- (a) all advertisements abide by the existing laws;
- (b) all advertisements show responsibility and protection of consumers;
- (c) all advertisements are decent, honest and truthful; and
- (d) there is conformity to the principles of fair competition in business

The UCC Advertising Standards lay down rules for advertisers, agencies and media owners. The standards contain a wide range of rules designed to ensure that advertising does not mislead, harm or offend. Advertisements must also be socially responsible and prepared in line with the principles of

fair competition. These broad principles apply regardless of the product, service and message being advertised.

In addition, the UCC Advertising Standards contain specific rules for certain products and marketing techniques. These include rules for telecoms advertising; alcoholic drinks, health and beauty claims, children, medicines, financial products and prize promotions. These rules are complimentary to existing laws and are subject to such laws as exist and or shall from time to time be enacted.

1.4 How is privacy law enforced in Uganda? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Both the courts and sector-specific regulatory bodies, such as the PDPO, under the NITA-U, enforce provisions of privacy law in Uganda. The DPPA provides for the establishment of the PDPO whose functions include overseeing the implementation and enforcement of the DPPA, the establishment and maintenance of the register of data controllers and data processors, and investigating any complaints relating to any purported infringement of any of the provisions of the DPPA, audit and promote awareness of privacy rights and obligations.

For examples of how the courts and the PDPO have enforced privacy law Uganda see question 10.3.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Uganda?

- (a) The Constitution is binding on all State organs and all persons. A company that processes personal data in ways that infringe constitutional privacy rights (eg, surveillance, disclosure without consent), it may be exposed to litigation.
- (b) Companies are required under the Companies Act to comply with other applicable laws, such as the DPPA, in how they manage and disclose information.
- (c) A company becomes subject to privacy law in Uganda as provided in the DPPA when it collects, processes, or stores personal data of individuals. Specifically:
 - (i) any company whether local or foreign which collects, processes, or stores personal data of Ugandans is subject to privacy law;
 - (ii) a company qualifies as a data controller or processor and is subject to privacy law;
 - (iii) a company must adhere to core data protection principles once it processes personal data. These principles include accountability, lawfulness and fairness, purpose limitation, data minimization, accuracy, security safeguards and consent; and
 - (iv) a company must register with the PDPO before collecting or processing personal data.

2.2 Does privacy law in Uganda apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the DPPA applies to foreign companies if they process the personal data of Ugandan citizens or residents, even if they operate from outside Uganda. Such companies must register with the PDPO and comply with all data protection obligations, including obtaining consent and ensuring secure data handling. While the law does not require a local representative, the PDPO may request a local contact person in practice. Non-compliance can lead to fines, enforcement actions, or prosecution.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Uganda?

Personal data is defined under the DPPA as: ‘information about a person from which the person can be identified, that is recorded in any form and includes data that relates to:

- (a) the nationality, age or marital status of the person;
- (b) the educational level, or occupation of the person;
- (c) an identification number, symbol or other particulars assigned to a person;
- (d) identity data; or
- (e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual’.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The DPPA identifies certain types of personal data, ie those relating to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status or medical records of an individual, as special personal data.

Such sensitive data is regulated more strictly, as processing such data requires explicit and informed consent from the individual. The consent must be specific, clear, and separate from general data collection.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

- (a) Anonymized data is generally not considered personal data and therefore not subject to regulation.
- (b) Pseudonymized data, however, is still treated as personal data and falls under the DPPA’s provisions.
- (c) De-identified data, while not explicitly defined in the Act, may be treated as personal data depending on the risk of re-identification.

The DPPA focuses on whether a person is identifiable, directly or indirectly, and does not provide detailed technical standards for anonymization or pseudonymization.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies must:

- (a) process personal data lawfully and transparently;
- (b) obtain informed consent from individuals;
- (c) collect only necessary and relevant data;
- (d) respect data subject rights including access, correction, and objection;
- (e) ensure data security;
- (f) register with the PDPO before processing data;
- (g) maintain proper records; and

- (h) ensure third-party processors are bound by data protection contracts. Cross-border transfers are restricted unless adequate safeguards are in place or consent is obtained.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

Yes, companies in Uganda are classified as data controllers or processors under the DPPA depending on their role in managing personal data:

- (a) A data collector is a person who collects personal data;
- (b) A data processor means a person other than an employee of the data controller who processes the data on behalf of the data controller.

Companies as data controllers have broader obligations: they determine why and how data is used, and must obtain consent, register, and ensure legal compliance.

Companies as processors handle data only on instructions from controllers and are mainly responsible for security and confidentiality.

Both controllers and processors must register with the PDPO and may be held liable for breaches depending on their level of control over the data.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes, the DPPA requires a lawful basis for processing personal data. The most common basis is informed consent, but other justifications include contractual necessity, legal obligations, protection of vital interests, and public interest tasks. Processing without a lawful basis is a breach of the Act and can result in enforcement action or penalties.

Collection and processing of special personal data is prohibited unless:

- (a) the information is given freely and with the consent of the data subject;
- (b) it is carried out by an employer in the exercise or performance of a right or an obligation conferred or imposed by law; or
- (c) it is for the purposes of the legitimate activities of a body or association which:
 - (i) is established for non-profit purposes; or
 - (ii) exists for political, philosophical, religious or trade union purposes; and
 - (iii) relates to individuals who are members of the body or association or have regular contact with the body or association in connection with its purposes, and does not involve disclosure of the personal data to a third party without the consent of the data subject.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The Companies Act does not directly address advertising, it reinforces the duty to operate lawfully and transparently in handling personal data.

The DPPA provides that companies as data processors and controllers processing personal data for advertising must provide privacy notices that clearly state:

- (a) the data controller's identity;
- (b) the purpose and type of data collected;
- (c) whether it will be shared;
- (d) the legal basis for processing;
- (e) data retention; and
- (f) individuals' rights including consent and opt-out options.

The UCC Advertising Standards further require consent for data use in marketing and clear opt-out mechanisms.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have the right to:

- (a) be informed;
- (b) give or withdraw consent;
- (c) object to direct marketing;
- (d) access and correct their personal data; and
- (e) seek redress if their data is misused in advertising.

These rights are protected under the DPPA, ensuring individuals retain control over how their personal data is used for marketing purposes.

The Uganda Communications (Consumer Protection) Regulations also offer additional protections that align with data privacy principles. These include protection from misleading or consent-less advertising, the right to clear information, and the enforcement of fair marketing practices especially in telecom and digital contexts. Therefore, these complement the rights guaranteed under the DPPA.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies must obtain consent before using personal data for advertising and must provide opt-out options for unsolicited marketing communications. These requirements are grounded in the DPPA and UCC Advertising Standards, which emphasize transparency, control, and user-friendly withdrawal mechanisms. Failure to comply may result in regulatory penalties or complaints to the PDPO.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

The DPPA regulates how personal data may be shared with and processed by vendors and third parties involved in advertising. Controllers must ensure that third parties such as ad agencies, DSPs, or data providers process data only under contract, with clear consent, and with appropriate safeguards and transparency. If data is transferred abroad or reused, stricter consent and protection measures apply.

Therefore, the Act places obligations on the data controller (the company initiating the advertising) to ensure data is handled lawfully, even when outsourced.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When companies disclose or receive personal data to or from vendors or other third parties, they are legally required under the DPPA to establish clear contractual obligations to protect that data.

Therefore, companies must enter into written contracts when disclosing or receiving personal data from third parties. These contracts must include obligations around:

- (a) purpose limitation;
- (b) security;
- (c) confidentiality;
- (d) sub-processing restrictions;
- (e) breach notification;
- (f) data return or deletion; and
- (g) compliance monitoring.

Cross-border data sharing requires additional safeguards or consent.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must undertake due diligence in their privacy practices by appointing a data protection officer ('DPO') if processing large volumes or sensitive data. The DPO:

- (a) manages and maintains records of data processing activities;
- (b) secures written contracts with third-party vendors;
- (c) ensures informed consent for advertising; and
- (d) enables individuals to exercise their data rights.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The DPPA sets out the rules for collecting, using, and storing personal data, and applies to businesses that collect and use consumer data for advertising and marketing purposes.

Direct marketing via email, SMS, or push notifications is strictly consent-based. Under the DPPA, explicit consent must be obtained before sending marketing messages and these messages must provide clear opt-out options. The UCC Advertising Standards reinforce this by prohibiting unsolicited messages and requiring consent for any targeted communication. Non-compliance may result in regulatory penalties from the PDPO.

SMS advertising is governed by guidelines issued by the Uganda Communications (Text and Multimedia Messaging) Regulations. These regulations came into force with the main objective of ensuring the fulfilment of essential requirements, including security of network operation, maintenance of network integrity, interoperability, data protection and protection of the environment. The Regulations:

- (a) promote the use, with confidence, of text and multimedia message by end users of communications services in Uganda, while minimizing encumbrances from mobile spam;
- (b) provide a transparent mechanism for complaints handling in relation to text and multimedia messaging, ensuring that complaints are handled in a fair and efficient manner;

- (c) establish a regime that ensures that reasonable steps are taken by authorized parties to protect children from viewing audiovisual content that is not suitable for them; and
- (d) ensure that the use of text and multimedia messages complies with the laws of Uganda.

The Computer Misuse Act enhances the protection of the right to privacy by addressing the issues arising from the misuse of online media including emails, push notifications and social media platforms.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The use of tracking technologies such as cookies, pixels, and SDKs is regulated under the DPPA. While the law does not name these technologies specifically, their use is governed through general provisions on data collection, consent, and transparency when personal data is involved.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no specific rules targeting loyalty programs. However, they must comply with the general principles of data protection when handling personal data particularly in regard to informed consent, transparency, data minimization, user rights, and third-party safeguards.

7.4 How is social media and influencer marketing regulated under privacy law?

Uganda does not have a law that specifically regulates social media and influencer advertising. The general laws apply. In particular:

- (a) The Computer Misuse Act provides for safe and secure use of computers in Uganda. It also creates offences for various matters. For instance, the Act provides that anyone who willfully and repeatedly uses electronic communication to disturb the peace or privacy of others with no purpose of legitimate communication will be guilty of sending an offensive communication. The Act also enhances the protection of the right to privacy by addressing the issues arising from the misuse of online and social media platforms; and
- (b) The Electronic Transactions Act Cap 99 provides for the use, security, facilitation and regulation of electronic communications and transactions, which could include commercial transactions on social media. It lays out the guidelines for information that should be provided by persons offering goods or services for sale, hire or exchange through an electronic transaction to consumers.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

The DPPA and the UCC Advertising Standards do not use the terms behavioral or personalized advertising explicitly. However, they impose clear obligations on the collection and use of personal data for such advertising, distinguishing it from contextual advertising, which does not rely on personal data.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not explicitly regulated by name under current law. However, their underlying activities such as the collection, matching, and sharing of personal data across platforms fall squarely under the DPPA. Therefore, these technologies are subject to strict obligations around consent, transparency, lawful processing, and security.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is regulated under the DPPA, which requires that informed consent be obtained before collecting or using an individual's location data.

Individuals must clearly be informed of the purpose of location tracking, how the data will be used (eg, for personalized ads), and whether it will be shared with third parties. Individuals have the right to object or withdraw consent at any time. Additionally, location data is considered sensitive personal data when it can reveal habits or movements, requiring stronger safeguards and data minimization practices.

7.8 How are data brokers defined and regulated under privacy law?

The term data broker is not defined and regulated under the DPPA.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children is firmly regulated to protect their personal data and well-being.

Under the DPPA, parental consent must be obtained before collecting or using a child's data to ensure that all marketing respects the child's best interests. The UCC Advertising Standards prohibit manipulative, unsafe, or misleading advertisements directed at minors. Together, these rules aim to ensure that children are not exploited or exposed to harmful advertising content.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The DPPA regulates profiling and the use of AI or automated decision-making for advertising by requiring a lawful basis—most commonly explicit consent—before collecting or using personal data for such purposes.

Individuals have the right to object to profiling and any automated processing that significantly affects them, such as targeting or segmenting for advertising.

The law emphasizes transparency, meaning companies must inform individuals:

- (a) if profiling or AI is being used;
- (b) the logic involved; and
- (c) the consequences of such processing.

Additionally, data minimization and security obligations apply to ensure only necessary data is used and properly protected during profiling or algorithmic advertising.

7.11 Are there other specific advertising practices that you wish to discuss?

Specific advertising practices are regulated under the DPPA and the UCC Advertising Standards. For example:

- (a) direct marketing requires opt-in consent, with clear opt-out options;
- (b) advertising to children demands parental consent and must avoid exploitative content;
- (c) influencers must disclose paid endorsements;
- (d) loyalty programs or prize promotions must be transparent, fair, and comply with data privacy rules; and
- (e) the use of tracking technologies such as cookies or pixels requires explicit consent and disclosure of their advertising purposes.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The DPPA provides for the processing personal data outside Uganda. Data can be transferred out of Uganda if:

- (a) the recipient country provides adequate protection;
- (b) the data subject gives explicit consent; or
- (c) standard contractual clauses or other legally binding safeguards are in place.

While the law does not list specific prohibited countries, in practice, transfers to countries with inadequate privacy protections must be mitigated through contractual mechanisms or explicit consent. Additionally, the PDPO may require prior approval or notification for high-risk international transfers.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Personal data transfers abroad require companies to:

- (a) ensure the data is used only for its original purpose and properly deleted or anonymized when no longer needed;
- (b) obtain informed consent from data subjects, especially when transferring to countries without adequate data protection; and
- (c) assess and mitigate risks associated with cross-border transfers, implementing safeguards such as encryption and access controls.

Additionally, transfers involving privileged or confidential information, such as legal or medical data, require heightened confidentiality measures and strict contractual protections to maintain privilege and prevent unauthorized disclosure.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Uganda? Are there minimum standards? Does this differ by sector or size of the entity?

The DPPA requires data controllers and processors to implement appropriate technical and organizational measures to protect personal data from unauthorized access, loss, or destruction. It mandates:

- (a) continuous risk assessments and adaptations to security safeguards as threats evolve;
- (b) adherence to ‘generally accepted information security practices,’ including sector-specific standards; and
- (c) notification of data security breaches.

These requirements apply universally, regardless of sector or organizational size. Nevertheless, the PDPO may provide sector-specific guidance, and expects all entities to designate a DPO and register their processing activities.

Non-compliance with these security obligations, such as failing to notify the PDPO of a breach, can result in fines, including up to 2% of annual turnover, and up to 10 years’ imprisonment for corporate officers who authorize breaches.

9.2 How are personal data breaches regulated in Uganda? What are the requirements for notification and response?

The DPPA requires immediate notification to the PDPO once a security breach is discovered. The PDPO will then determine whether the data controller, data collector or data processor should notify the data subject of the breach, which notification shall be made by:

- (a) registered mail to the data subject's last known residential or postal address;
- (b) electronic mail to the data subject's last known electronic mail address;
- (c) placement in a prominent position on the website of the responsible party; or
- (d) publication in the mass media,

providing sufficient information relating to the breach to allow the data subject to take protective measures against the consequences of unauthorized access or acquisition of the data.

Where the PDPO has grounds to believe that publicity would protect a data subject affected by the unauthorized access or acquisition of data, it may direct the responsible party to publicize the breach in a manner specified by the PDPO.

The DPP Regulations further stipulate that breach notifications must detail:

- (a) the nature of the data involved;
- (b) the number of affected individuals;
- (c) the likely consequences; and
- (d) the remedial measures taken.

While the PDPO determines whether affected individuals must also be informed, it requires companies to do so if harm is likely. Failure to report a breach can lead to penalties, including fines and possible criminal sanctions.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

The DPPA prohibits unlawful obtaining or disclosure of personal data, unlawful destruction or alteration of data, and sale of personal data. These violations carry penalties of up to 245 currency points or up to 10 years' imprisonment, or both.

If a corporation commits one of these offences, both the company and any officers who knowingly authorize the breach are liable, and the court may impose fines of up to 2% of the corporation's annual gross turnover, in addition to individual penalties.

Furthermore, the PDPO can issue orders to remedy breaches and data subjects are entitled to claim compensation for damage or distress under

The DPP Regulations state that failure to comply with security notification obligations, processing without consent, or obstructing investigations may also trigger enforcement actions, including deregistration and further fines.

10.2 Do consumers have a private right of action? What remedies are available to them?

Consumers have a private right of action under the DPPA, which allows them to seek redress when their data protection rights have been violated. Individuals can formally complain to the PDPO if they believe their rights have been infringed. Individuals are entitled to claim compensation for any damage or distress caused by processing which breaches the Act. Finally, if internal resolution is unsuccessful, consumers can go to court and seek declaratory and injunctive remedies, as well as damages and costs.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement of privacy laws in advertising is growing slowly:

- (a) In 2023, the PDPO concluded an investigation against Uganda Securities Exchange ('USE') and Soft Edge Uganda Limited for violations of the DPPA following a security breach. Unauthorized access to USE's logging servers exposed personal data due to a misconfigured firewall, and USE failed to detect a Twitter message about the breach, allowing it to continue for 12 days. The PDPO found that the agreement between USE and Soft Edge Uganda was inadequate in securing data integrity and confidentiality, and Soft Edge Uganda was not registered with the PDPO. The PDPO decided that USE and Soft Edge Uganda should be prosecuted for negligence and gave them three months to rectify non-compliant actions, urging USE to initiate disciplinary proceedings against involved personnel.
- (b) In 2021 NITA-U conducted investigations (following a complaint brought to the attention of the Speaker of Parliament by Unwanted Witness) into concerns of unlawful data sharing by Safeboda. The investigation found Safeboda had unlawfully disclosed user data to analytics company CleverTap without prior informed consent, breaching the DPPA. As a result, SafeBoda was ordered to revise its privacy notices, obtain explicit consent for data sharing, and improve its data breach and access processes.
- (c) The High Court of Uganda, in *Nalubega Shadia v Stabex International Ltd*, found that the defendant violated the plaintiff's privacy rights and infringed her personality and image rights under the DPPA, as well as the Constitution. The court concluded that the unauthorized use of her photographs for promotional materials without her informed consent constituted unlawful processing of her personal data. As a result, Stabex was ordered to cease using her images and pay UGX 5 million in damages.
- (d) In February 2024, AdLegal Uganda filed a privacy-related complaint with UCC against Airtel Uganda, alleging that the company's use of social media influencers to promote services without proper disclosure of paid advertising violated privacy regulations. Airtel denied the accusations, but UCC acknowledged a regulatory gap, as its existing advertising standards do not specifically address influencer marketing. As of mid-2025, the matter remains under investigation by the UCC, with no formal determination concluded. This case highlights the need for updated regulations to cover digital advertising practices, particularly those involving social media influencers.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Uganda?

Ugandan privacy law doesn't explicitly codify cultural norms, but communal values and respect for family unity influence how privacy is understood and enforced, especially under the Constitution of Uganda, and the DPPA. These provisions emphasize informed consent and lawful processing, which must be sensitive to cultural contexts, particularly regarding tribal affiliation, customary practices, or family data, where communal well-being often takes precedence.

The UCC Advertising Standards also require that ads take into account public sensitivity and social norms, reflecting Uganda's cultural emphasis on shared values and respect for elders. Combined, these laws require that both data controllers and advertisers take into account cultural norms, especially in rural or traditional settings, to ensure that privacy practices align with community customs and avoid causing social harm.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

In Uganda, several emerging hot topics are shaping how companies approach privacy and advertising compliance. These include:

- (a) The rise of AI, machine learning, and big data which brings significant challenges under the DPPA, particularly around profiling, transparency, fairness, and liability. The DPPA sets out the need for informed consent, purpose limitation, and rights to object;
- (b) The integration of digital identity systems, such as national ID databases or SIM-linked identifiers, raises concerns about informed consent, data linkage, and surveillance, especially given the lack of AI-specific amendments in the DPPA;
- (c) Influencer marketing and embedded advertising present new regulatory gaps within the UCC Advertising Standards, increasingly attracting complaints about undisclosed paid content;
- (d) Lastly, cross-border data flows and the development of data clean rooms pose legal challenges, as entities will need robust transfer mechanisms like standard contractual clauses and adherence to the provisions of the DPPA for security and third-party contracts. Companies should also monitor ongoing efforts to update and amend the DPPA to better address these issues, including possible AI-specific regulations.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Beyond the areas covered, companies in Uganda should be mindful of broader regulatory convergence and emerging enforcement trends:

- (a) The forthcoming NITA-U Regulations may introduce explicit data breach notification timetables, privacy by design requirements, and mandatory DPOs for medium-sized enterprises expanding the obligations already found in the DPPA;
- (b) Under the UCC Advertising Standards, operators of digital platforms and social media must prepare for stricter oversight of influencer disclosures, embedded advertising, and platform liability relating to privacy violations;
- (c) Additionally, as blockchain and biometric ID systems like SIM registration are more widely deployed, companies must pay attention to both the DPPA and the SIM Card Registration Regulation 2016 to ensure lawful collection and use of sensitive and identity data; and

- (d) Regional developments, such as the African Union’s Model Law on Data Protection and its linkage to the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), are likely to influence Uganda’s data protection reforms. As a result, the provisions of the DPPA related to cross border data transfers and vendor oversight will have increasing relevance in a harmonized East African data environment.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Since 2022, Uganda’s privacy landscape has evolved significantly, driven largely by rapid technological innovation and national security measures:

- (a) In January 2024, Parliament’s call to amend the DPPA especially to address AI and machine learning highlights renewed focus on the provisions concerning consent, profiling, and automated decision-making;
- (b) The government’s rollout of license plate tracking and CCTV networks under the Regulation of Interception of Communications Act Cap 101 has sparked privacy and surveillance concerns, particularly in light of the provisions of the DPPA on preventing unjustified collection of personal data;
- (c) The UCC Advertising Standards and broader consumer transparency mandates are also under review, with growing attention on influencer marketing disclosures; and
- (d) Biometric SIM registration linked to national ID cards continues expansion, raising data linkage and consent issues governed by the DPPA, and these developments are prompting calls for clearer breach notifications, privacy-by-design, and sector-specific guidance from the PDPO.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Companies in Uganda have faced growing challenges in keeping up with evolving privacy demands amid rapid technological expansion. The PDPO is actively monitoring compliance, but enforcement remains hindered by limited resources, low public awareness, and lack of detailed regulations, particularly for breach notifications under the DPPA. This enforcement gap has allowed organizations, including telecom networks and government agencies, to quietly collect sensitive data like biometrics and national IDs for SIM registration and surveillance systems, raising concerns according to the DPPA’s limits on unjustified data processing. Additionally, firms are navigating emerging advertising challenges, such as influencer disclosures and targeted ads compliance, under the UCC Advertising Standards while lacking formal guidance on novel modalities such as AI-driven advertising. Finally, low consumer trust and weak compliance culture, exacerbated by loopholes in cross-border data sharing rules under the DPPA, are driving calls for sector-specific regulations and more detailed standards from both the PDPO and other regulators.

12.3 What do you envision the privacy landscape will look like in five years?

Over the next five years, Uganda’s privacy landscape is expected to undergo significant transformation, driven by regulatory maturity, technological adoption, and increasing public awareness.

First of all, the DPPA is likely to be amended to address current gaps particularly around AI, automated decision-making, and cross-border data transfers which are not yet fully regulated under the existing legal framework.

Secondly, there is anticipated growth in enforcement capacity by the PDPO, with more sector-specific guidelines, mandatory breach notification procedures particularly in areas like telecommunications, health, finance, and digital marketing. Simultaneously, consumer awareness is likely to grow, leading to more data subject complaints and legal challenges particularly in response to profiling, targeted advertising, and biometric data collection practices (eg. SIM card registration or digital ID systems).

Lastly, regional legal harmonization, spurred by the African Union's Model Data Protection Law and East African Community ('EAC') policy frameworks, will push Uganda to align with broader continental standards. Companies will need to invest in privacy governance, compliance infrastructure, and ethical tech use to meet rising expectations, especially as digital services expand and new tools like facial recognition, digital wallets, and clean room technologies become more common.

UKRAINE

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Ukraine.

The current Ukrainian legislation is mainly based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') and the EU Data Protection Directive, from which basic concepts are borrowed, such as rights and obligations of data subjects, controllers and processors, legal bases for data processing and cross-border data transfers, etc.

Led by the commitments in the Association Agreement with the European Union in October 2017, the Ukrainian Parliament plan to implement the regulations of the EU General Data Protection Regulation ('GDPR') into national legislation. However, this goal has still not been achieved, although there have been several unsuccessful attempts to draft an implementation bill. Notably, the Parliament of Ukraine has resumed consideration of Draft Law No 8153 on Personal Data Protection ('Draft Law'). In November 2024, the Draft Law was adopted as a basis in the first reading and is currently undergoing further refinement before the second reading.

The legal enforcement of data privacy rights in Ukraine is still not as strong as, say, in the European Union. The appetite of data subjects to go to court is also much lower than in other countries. Although the awareness of data privacy has increased within certain industry sectors (eg, IT and telecommunications), Ukrainian business is quite reluctant to implement self-regulating mechanisms.

1.2 What are the primary laws regulating privacy in Ukraine? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The Constitution of Ukraine dated June 28, 1996 establishes the fundamentals of privacy in Ukraine.

Privacy rights are further expanded in the Law of Ukraine on Personal Data Protection dated June 1, 2010 ('Privacy Act'). The Privacy Act is the principal source of regulation of data privacy issues and contains the most important legal provisions in this sphere. In addition, there are numerous applicable by-laws and regulations. Ukraine is also a signatory to Convention 108. However, none of these contain specific rules to cover privacy issues with special focus on advertising aspects.

Ukraine has also adopted several sector-specific laws containing privacy rules (eg, the E-commerce Act, the Electronic Communications Act, and the Media Act). The Advertising Act establishes the rules for conducting advertising via electronic communications.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

We are not aware of any self-regulatory bodies having been created in Ukraine in the field of data protection, particularly with a focus on privacy issues in advertising. However, four self-regulatory bodies have been incorporated and registered in the fields of audio, audiovisual, printed and online media, of which the audiovisual self-regulatory body appears to be the most active. The National Council of Television and Radio Broadcasting has already commenced elaborating a Code on creating and disseminating information based on the current legal framework. We expect that some privacy-related issues in advertising activity may be incorporated into Codes such as this. In the meantime, non-government organizations are actively involved in the process of public discussion of both international and national best practices in the field of data protection.

1.4 How is privacy law enforced in Ukraine? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The central competent data privacy authority is the Ukrainian Parliament's Commissioner for Human Rights ('Ombudsman'). The Ombudsman is in charge of overseeing compliance with the Privacy Act. To this end, the Ombudsman has powers including, inter alia, to consider complaints from data subjects, to carry out inspections (either scheduled or unscheduled), and to impose administrative sanctions on the violators, including fines.

The sanctioning powers of the Ombudsman are rather limited. In most cases, the Ombudsman decides to issue a warning notice to the violator to cease the violation or to rectify defects in processing practices. Even if the Ombudsman decides to impose a fine on the violator, such fine is likely to be very insignificant in monetary terms.

A violation of the Ukrainian privacy laws may also result in civil, administrative or even (in very rare cases related to illegal collection and distribution of personal data) criminal liability.

There are several other state bodies which have limited privacy enforcement powers in certain industries (eg, the telecoms regulator and the consumer protection authority).

As yet, there is no known enforcement practice originated by self-regulatory bodies in Ukraine.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Ukraine?

The Privacy Act does not contain any express provisions regarding its territorial effect. As a general rule, all companies and organizations dealing with data processing activities within Ukraine are subject to privacy laws in Ukraine.

However, there are some excluded subject matters where provisions of the Privacy Act are not applicable. Specifically, personal data processing may be carried out without applying the provisions of the Privacy Act where such processing is carried out:

- (a) by a natural person exclusively for private and household purposes; and
- (b) exclusively for journalistic and artistic purposes, provided that the balance between the freedom to express thoughts and a person's right to private life is ensured.

2.2 Does privacy law in Ukraine apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The Privacy Act does not contain a clear provision addressing the issue of jurisdiction. However, the laws of Ukraine do not claim to have an extraterritorial effect in other countries. Therefore, companies based or operating outside of Ukraine may only be subject to the Ukrainian data protection regime to the extent that they process personal data in Ukraine. An entity with a physical presence in Ukraine (through a local branch office, with or without employees) is within the scope of the Privacy Act even if the personal data that is processed in Ukraine relates to foreign individuals.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Ukraine?

The Privacy Act defines ‘personal data’ as data or an aggregate of data on an individual who is identified or can be precisely identified.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Privacy Act names the following types of personal data to be sensitive:

- (a) race, ethnic origin;
- (b) political, philosophical and religious beliefs;
- (c) membership of political parties and trade unions;
- (d) health;
- (e) sexual life;
- (f) biometric data;
- (g) genetic data; and
- (h) criminal convictions.

In turn, regulations of the Ombudsman regard all the above as ‘extreme risks personal data’ with the addition of:

- (i) nationality;
- (j) membership in religious organizations, or worldview-oriented public organizations;
- (k) administrative liability;
- (l) any pre-trial procedures;
- (m) any investigative procedures against the data subject;
- (n) violence against the data subject; and
- (o) the data subject’s location and travel (movement) routes.

The Ombudsman should be notified within 30 days of commencing extreme risk personal data processing. No other notifications, registrations, authorizations, etc, are currently required to be made to/filed with the Ombudsman, not even notifications of any data breach or cross-border data transfer. Once extreme risk personal data is processed, it is also necessary to notify the Ombudsman as to a company’s data processing division or of the appointment of a data protection officer. Such notification can be filed simultaneously with the notification of extreme risk personal data processing. These notifications are not required if processing the extreme risk personal data falls within a statutory exemption (see question 4.3).

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

- (a) **Anonymization of personal data** in Ukraine, in contrast to the European Union, where the definitions of ‘processing of personal data’ and ‘processing’ in the EU Data Protection Directive and the GDPR respectively do not cover such processing, is covered by the definition of ‘personal data processing’ in the Ukrainian Privacy Act. It therefore generally requires the consent of a data subject unless it is possible to rely on another legal basis/derogation (see question 4.3). However, once personal data has been anonymized, any further processing of the anonymized data, including for analytical purposes, does not require any specific/additional grounding (legal basis).

Key considerations regarding anonymization include:

- (i) **purpose limitation and data minimization:** The data controller must clearly define the purpose of the data collection/processing, define the scope of personal data to be processed, and ensure that the collected data is processed strictly for the defined purpose;
- (ii) **implementing technical anonymity measures** to ensure that the tools and platforms used for data collection do not capture individual identifiable information (in aggregate), such as IP addresses, device IDs, or other technical markers that could link responses to specific individuals;
- (iii) **assessing the anonymization** in order to evaluate whether the methods applied to anonymize the data are robust and account for all reasonably foreseeable means of identifying an individual. This includes assessing the likelihood of identification by third parties if the data is shared;
- (iv) **transparency** (and data subject's consent if consent is a legal basis for collecting and further anonymization of personal data): While not strictly required for anonymous data, it is recommended to inform data subjects of the measures taken to ensure anonymity, and how the data will be used; and
- (v) **third-party involvement:** If third parties (eg, survey providers, marketing specialists, external consultants, etc) are involved in data collection or processing, it is important to ensure that they comply with data protection requirements, including by signing agreements to guarantee that no personal data is traceable or identifiable.

Anonymous data does not constitute 'personal data' under the Privacy Act, as it cannot be used to directly or indirectly identify an individual.

- (b) **Pseudonymized data** (eg, replacing names with pseudonyms and decryption keys) can be treated as not fully anonymous and may, therefore, be subject to the Privacy Act (through it should be assessed on a case-by-case basis). While pseudonymization reduces the risk of re-identification, it can still facilitate compliance with data protection obligations.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The privacy laws in Ukraine do not contain dedicated provisions setting out the principles for personal data processing. Instead, such principles are set out in different provisions, mostly in the Privacy Act. These principles include the following:

- (a) **transparency**—personal data must be processed lawfully, fairly and in a transparent manner;
- (b) **lawful basis for processing**—personal data may be only processed if it falls within the grounds for processing envisaged by the Ukrainian laws (see question 4.3);
- (c) **purpose limitation**—processing of personal data must be carried out only for the specified, explicit and legitimate purpose known to the data subject;
- (d) **data minimization**—the data must be adequate, relevant and limited to what is necessary in relation to the purpose of the processing;
- (e) **retention (storage limitation)**—data should be kept no longer than it is necessary for the purpose for which such personal data is being processed;

- (f) **data security**—the entity engaged in processing data must ensure appropriate security measures are in place to protect personal data; and
- (g) **accuracy**—personal data should be accurate and up to date.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

The Privacy Act names controllers, processors and third parties as the main actors engaged in personal data processing. The concepts of ‘controller’ and ‘processor’ in Ukraine are almost identical to those existing in EU legislation.

There is no absolutely clear position as regards the status of ‘third parties’ in terms of personal data processing. According to the Privacy Act, a ‘third party’ may be any person receiving personal data from a controller or processor. In practice, a third party is usually regarded as a potential recipient of personal data provided by the data controller or data processor. A third party in receipt of the respective data may acquire the status of a separate data controller or data processor. Note that, unlike many other jurisdictions, sub-processor and joint controller roles are not expressly regulated under the Ukrainian law.

In general, controllers bear primary responsibility for ensuring that processing activities are compliant with Ukrainian privacy laws. In particular, a party transferring personal data (ie, a data exporter) must ensure compliance with the conditions of the established regime for personal data protection.

The controller may involve a data processor in the processing activities. Ukrainian law requires a written agreement between the controller and the processor. However, unlike the GDPR, Ukrainian law does not prescribe minimum content and requirements concerning this agreement.

Under the Privacy Act, the obligations of controllers and processors in terms of processing activities are almost the same, apart from some specific obligations, including notification requirements (for controllers) and compliance with controller’s instructions (for processors).

4.3 **Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

The Privacy Act mandates that the processing of personal data must be based on a lawful ground. Specifically the processing of:

- (a) **general personal data** is permissible if one of the following legal bases is met:
 - (i) consent of the personal data subject to the processing of their personal data. Note that consent under must be provided in written form or in any other format that allows for the unequivocal determination that consent has been granted. This provision expressly recognizes the validity of consent given in electronic form;
 - (ii) permission to process personal data is granted to the data controller in accordance with the law solely for the exercise of its powers;
 - (iii) the conclusion and execution of a transaction (contract) to which the personal data subject is a party, or which is concluded in favor of the personal data subject or taking actions prior to the conclusion of a contract at the demand of the personal data subject;
 - (iv) the protection of the personal data subject’s vital interests;
 - (v) the requirement to fulfil the data controller’s obligation, which is provided for by law;
- or

- (vi) the requirement to protect the legitimate interests of the data controller or a third party to whom the personal data is transferred, except where the requirement to protect the fundamental rights and freedoms of the personal data subject in connection with their data processing takes precedence over such interests.
- (b) **sensitive personal data** (see question 3.2) is subject to stricter requirements and is permitted only under specific legal grounds, including:
 - (i) an explicit consent from the data subject;
 - (ii) processing is necessary for the purposes of carrying out the obligations and rights of the data controller in the field of employment law in so far as it is authorized by law providing for adequate safeguards;
 - (iii) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving their consent;
 - (iv) processing is carried out with appropriate guarantees by a religious organization, ideological NGO, political party or trade union established according to the law provided that the processing relates solely to the members of such organization/party/union or to persons who have regular contact with it in connection with its purposes and that personal data are not disclosed to a third party without the consent of the data subjects;
 - (v) processing is necessary for the establishment, exercise or defense of legal claims;
 - (vi) processing is necessary for the purposes of healthcare, medical diagnosis, care or treatment or provision of medical services carried out by the statutory specified subjects;
 - (vii) processing is necessary for the purposes of military registration of conscripts and reservists;
 - (viii) processing relates to court verdicts, performing pre-trial or counter-intelligence procedures, combating terrorism and is performed by the state authorities within their powers established by law; or
 - (ix) processing relates to data which is manifestly made public by the data subject.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

The Ukrainian privacy law landscape does not envisage specific obligations as regards privacy in terms of advertising. However, general obligations under privacy laws should be followed. Those include, among others:

- (a) **Notification requirement**—to notify the data subject in relation to personal data collection on the day of the collection (if collected from the data subject) or within 30 business days after collection (in all other cases). The data subject should be notified regarding:
 - (i) the data controller (eg, name and registered address),
 - (ii) the scope (categories) of the personal data collected,
 - (iii) the rights of the data subject under the law,
 - (iv) the purpose of personal data collection, and
 - (v) third parties to whom its personal data can be transferred;

- (b) **Security requirement**—controllers and processors to undertake adequate security measures as regards processed personal data;
- (c) **Recording requirements**—controllers and processors to track the operations related to personal data processing. The Master Template of the Personal Data Processing Procedure ('Master Template') approved by the Ombudsman states that, where personal data is processed by an automated system, such system must automatically record the following information on personal data processing:
 - (i) date, time and source of collection of personal data of a data subject,
 - (ii) alteration of personal data,
 - (iii) viewing of personal data,
 - (iv) any transfer (copying) of personal data of a data subject,
 - (v) date and time of personal data deletion or erasure,
 - (vi) details of persons who made any of the above actions, and
 - (vii) purpose and reasons for alteration, viewing, transfer, deletion or erasure of personal data.

This information must be stored by the data controller/processor for one year.

The Master Template is generally considered not to be binding. However, the Procedure of Conducting Control over Compliance with the Personal Data Protection Laws by the Ombudsman mentions the Master Template as being one of the documents which the Ombudsman considers when conducting its inspections with respect to compliance with Ukrainian personal data protection laws. Therefore, it is usually advisable to generally comply with the Master Template.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

According to the Advertising Act, the main principles to which advertising must adhere are: lawfulness, accuracy, and the use of forms and means that do not cause damage to consumers of advertising. In addition, advertising must not undermine society's credibility and must be in line with principles of fair competition.

The Advertising Act itself does not establish a specific list of consumers' rights from an advertising perspective. Data subjects' rights are listed in the Privacy Act. These include:

- (a) the right to know the source and place of storage of their personal data, the purpose for which it is being processed, and address of the controller or processor;
- (b) the right to information on the conditions of access to their personal data, including information on the third parties to whom personal data are transferred;
- (c) right to receive a response to a request as to whether their personal data is stored in a database, and to receive the content of such data, within 30 days after receipt of the request;
- (d) right to object to the processing of their personal data;
- (e) right to request the alteration or destruction of their personal data if processed illegally or the data are inaccurate;
- (f) right to have their data protected;
- (g) right to complain or seek legal redress;
- (h) right, when granting consent, to make reservations to restrict the right to process their personal data;
- (i) right to withdraw consent; and

- (j) right to be informed of the procedure for automated processing of personal data, and the right to be safeguarded against an automated decision having legal implications for them.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Under the Advertising Act, it is prohibited to disseminate advertising in the form of spam, including conducting mass calls with the use of any technologies and communications, including in electronic form, without prior written consent of the consumer. Advertising by phone numbers or the other network identifiers may be conducted only based on prior written consent (which may be in electronic form) of the consumer concerned, and the consumer must be able to subsequently refuse having their data used—including refusal to receive advertising with the use of phone numbers or other network identifiers—by means of a plain and clear form on a free-of-charge basis. The same legal provisions are contained in the E-commerce Act regarding commercial electronic messages (see question 7.1(a)).

In practice, advertising disseminators incorporate an ‘unsubscribe’ button/link into the email footer in order that consumer can exercise its above-mentioned right and stop receiving advertising, newsletters or other marketing materials. Alternative methods are provided for text messages etc.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

- (a) Currently, there are no specific data privacy regulations governing the use of advertising agencies, demand-side platforms, supply-side platforms, data providers, or other vendors and third parties in advertising. Instead, general data protection requirements apply, including:
 - (i) **ensuring lawful data processing:** obtaining user consent where required or relying on another lawful basis for processing (see question 4.3);
 - (ii) **contractual safeguards:** entering into written data processing agreements (‘DPA’s) with vendors and third parties to outline data protection obligations;
 - (iii) **transparency and data subject rights:** informing data subjects about third-party involvement in data processing through privacy policies and ensuring compliance with data subjects’ rights, including such as access, deletion, and opting out of data transfers; and
 - (iv) **data transfer restrictions:** implementing safeguards for cross-border data transfers to countries lacking adequate level of data protection. Unlike the EU, which has long-established standard contractual clauses (‘SCC’s), Ukraine has not yet introduced standardized personal data protection terms, apart from the existing lawful bases.
- (b) However, the Draft Law (see question 1.1) aims to align Ukraine’s framework on personal data protection more closely with GDPR standards. Specifically, for transfers to jurisdictions without an adequate level of data protection, the Draft Law proposes additional mechanisms beyond the existing, case-by-case legal bases, including:
 - (i) a legally binding and enforceable instrument between public authorities;
 - (ii) binding corporate rules;
 - (iii) an approved code of conduct;

- (iv) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and
- (v) standard personal data protection terms approved by the Ombudsman (it could be that the Draft Law means the standard contractual clauses similar to the GDPR).

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

The dissemination of personal data is considered a transfer of information for which the consent of the data subject is required. The duty to fulfil the requirements for personal data protection is upon the party who disseminates the personal data. The receiving party shall take actions in advance with regard to the requirements of the Privacy Act.

In line with the Privacy Act, the data controller may entrust data processing to a data processor in accordance with a written agreement. The data processor may process personal data only within the scope and for the purposes stipulated in the agreement. In practice, the disclosing and receiving parties incorporate contractual provisions into the agreement whereby the receiving party undertakes to ensure the proper level of protection of disclosed data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

There are no specific statutory requirements related to processing personal data for advertising uses. As a rule, the parties must comply with general statutory rules on processing personal data. Data controllers, data processors, as well as third parties, must ensure protection of personal data from unauthorized processing, including its loss, accidental or illegal destruction, as well as from unauthorized access.

When it comes to due diligence measures, the Ombudsman's guidance on processing personal data based on the consent of data subject is a useful tool to check whether all aspects of processing of personal data are covered. In particular, in order to provide an informed consent, a data subject must have been provided with answers to the following questions:

- (a) who will process its personal data? (ie, the name of data controller, its address, contact number etc);
- (b) what is the purpose of processing personal data? (this must be accurate and understandable);
- (c) what is the scope of personal data subject to processing? (clear and exhaustive list of personal data intended to be processed);
- (d) what actions will be performed on the personal data in the course of processing? (ie, collection, storage, transfer, anonymization etc);
- (e) what is a data processor? What rights and does it have within the course of processing personal data?
- (f) who can receive personal data? The grounds and reasons for receiving personal data.
- (g) how long will personal data be processed?

along with a statement on withdrawal of the consent for processing personal data and the consequences thereof and of the other rights of data subjects under the Privacy Act (see question 5.2).

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

Ukrainian law does not define or regulate in detail the marketing communications. The following general rules may apply:

- (a) **E-commerce Act:** The E-commerce Act defines ‘commercial electronic messages’ (solicitation letters) as electronic messages in any form whose purpose is the direct or indirect promotion of goods, work or services, or business reputation of a person who carries out commercial or independent professional activity.

Addressee’s consent to receive electronic commercial messages is required with one exception—namely, commercial electronic messages may be sent to addressees (eg, potential buyers) without their express consent (which may be given in electronic form), provided that the addressee has the opportunity to unsubscribe from further receiving such messages. A data subject’s consent may be obtained during their registration in an e-commerce entity’s information and telecommunications system. Specifically, consent may be given by means of ticking a checkbox that indicates the data subject’s agreement to the processing of their personal information for a specified purpose, provided that the system does not allow for the processing of such personal information before the checkbox is ticked.

A commercial electronic message must comply with the following requirements:

- (i) it must be clearly identified as a commercial electronic message;
- (ii) the person on whose behalf the commercial electronic message is sent must provide recipients with direct and easy access to details of the seller/service provider;
- (iii) commercial electronic messages regarding rebates, premiums and prizes, etc, must be clearly indicated as such, and conditions of their receipt must be available and worded in such a way as to avoid ambiguity as well as comply with advertising laws requirements; and
- (iv) information about the cost of the goods, works and services must include information as to whether applicable taxes are included and (in the case of supply of goods) delivery costs.

The E-Commerce Act expressly prohibits the practice whereby the receipt of a commercial electronic message by a consumer without their consent is used as a reason for increasing service fees charged by telecom operators/providers, payment system operators, hosting providers, Internet access providers, etc.

- (b) **Advertising Act:** The Advertising Act establishes specific requirements regarding the promotion of services via means of electronic communication (including, telecommunications), which arguably also includes advertising on the internet and social media. Such advertising must contain the following details:
 - (i) description of the service;
 - (ii) service fee;
 - (iii) age or other restrictions for customers;
 - (iv) information about telephone call charges (paid or free of charge) when rendering the service, and the price of a one-minute call; and
 - (v) full name and address of service provider.

The font size for the above information should not be smaller than half the size of the font used for the telephone number used for rendering the services.

Distribution of advertising via telex or fax is expressly prohibited.

The Advertising Act places a direct prohibition on the disseminating of messages concerning the advertisement of alcoholic beverages and tobacco, their trademarks and other intellectual property rights used for the production of alcoholic beverages and tobacco, to an unspecified number of recipients via post, emails or mobile phones.

- (c) **Electronic Communications Act:** Effective as of January 1, 2022, the Electronic Communications Act provides a definition of ‘spam’ as electronic, text, and/or multimedia messages that are repeatedly (more than five messages per subscriber) sent to users’ email addresses or terminal equipment, without their prior consent. Dissemination of spam is prohibited.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Ukrainian law does not specifically regulate the use of tracking technologies. Where advertising and targeting cookies are used, compliance with the Privacy Act is crucial to mitigate risks related to violations of consumer protection laws—such as the solicitation of goods and services without consent. Ensuring transparency, for instance, by clearly disclosing the use of cookies for targeted advertising purposes in a cookie policy, also helps maintain compliance with anti-spam regulations.

7.3 How are loyalty programs and promotions regulated under privacy law?

If a data subject’s personal data is collected and processed as a condition to participating in a loyalty program/promotion, the loyalty program/promotion’s official terms must contain provisions relating to obtaining (informed) consent from the data subject (ie, it must set out, among other matters, the specific purpose of the personal data processing and the scope of the processed personal data). This includes ensuring prior written consent (including in electronic form) for advertising via phone numbers or other network identifiers, with a simple and clear opt-out mechanism.

Notably, the continuous sending of telephone, fax, electronic, or other messages without the consumer’s consent is prohibited as an aggressive form of commercial practice.

7.4 How is social media and influencer marketing regulated under privacy law?

- (a) **Social media marketing:** Marketing or advertising on platforms for shared access to information and platforms for shared access to video (social network services), if displayed to individuals located in Ukraine, is generally subject to the requirements of the Privacy Act. Providers of such platforms are prohibited from processing children’s and minors’ personal data for commercial purposes such as direct marketing and profiling, including behaviorally targeted advertising. There is general prohibition under the Media Act on the commercial use of children’s and minors’ personal data.

Marketing/advertising in social media must comply with the Advertising Act if:

- (i) the social media is located within a Ukrainian segment of the Internet (eg, registered in domain ‘UA’);
- (ii) customers targeted by such advertising are located in the territory of Ukraine; or
- (iii) the advertising is placed by technical means located in the territory of Ukraine.

- (b) **Influencer's marketing:** With effect from October 2023, the amended Advertising Act provides regulation for online advertising distributed within influencer's content. The amendments aim to align the Ukrainian advertising law with the legislation of the European Union, specifically the European Convention on Transfrontier Television, and the Audiovisual Media Services Directive (2010/13/EU) as amended by Directive 2018/1808/EU.

The Advertising Act applies to influencer marketing or advertising which qualifies as 'user-generated content' and, where relevant, 'product placement' or 'sponsorship'. Subsequently, if influencers (bloggers) voluntarily register as online media under the Media Act (gaining benefits such as eligibility for state grants and procurements, official journalist status, participation in co-regulatory bodies, enhanced legal protection, and lightweight penalties), they become subject to online media regulation under the Advertising Act.

Overall, influencers are now held to the same limitations related to advertising content as all other advertisers.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

The general rules outlined above (see question 7.1) apply. Although the Advertising Act references 'behaviorally targeted advertising', it does not define it.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Ukraine does not have specific regulations explicitly addressing digital identity resolution and clean room technologies. However, these technologies may still be subject to existing privacy laws, particularly the Privacy Act.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising typically requires the explicit consent of the individual. The consent must be freely given, specific, informed, and unambiguous. Data subject must opt in to location tracking and location-based advertising, with the option to withdraw consent at any time. When it comes to explicit consent in the Internet environment, a 'double opt-in' is usually advisable for the explicit consent, (ie, an additional confirmation from data subject is needed).

If location-based advertising entails the processing of precise location and movements of route, a notification to the Ombudsman for processing of such data must be made. However, if the location data is general and does not enable the identification or tracking of an individual's specific movements or routes (eg, data that only provides an estimated region or city), it may be considered non-sensitive and require only the simple consent of data subject.

7.8 How are data brokers defined and regulated under privacy law?

Ukrainian law does not regulate the activities of data brokers. The general rules and regulations apply.

Breaches involving private or restricted-access information may incur criminal penalties pursuant to the Criminal Code.

7.9 How is advertising to children and minors regulated under privacy law?

The Privacy Act does not establish specific rules for processing personal data of children and minors. Recent changes to the Advertising Act have placed certain restrictions on processing the personal data of children and minors. Specifically, subjects in the field of audio and audiovisual media may not process the personal data of children for direct marketing and profiling, including behavioral advertising. The same restriction applies to providers of platforms for shared access to video, and platforms for shared access to information.

Particular consideration must be given to the privacy rules governing advertising targeted at children, who represent the most susceptible demographic in comparison to adult audiences. In this regard, the Advertising Act expressly prohibits:

- (a) the use of images of children consuming or utilizing products intended exclusively for adults or those legally restricted from purchase or consumption by minors;
- (b) featuring children in hazardous situations or circumstances that, if imitated, could pose a risk to their well-being or that of others. Additionally, advertising must not contain content that encourages a dismissive attitude toward situations that are dangerous to health and life; and
- (c) television commercials (teleshopping) encouraging children to enter into sales or rental agreements that may require them to provide personal data necessary for completing the order.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Ukrainian privacy law does not have a dedicated regulation explicitly governing profiling, artificial intelligence, or automated decision-making in advertising. However, these activities fall under the general framework of personal data protection and related legal principles, particularly the Advertising Act and Privacy Act.

Notably, the rights of data subjects under the Privacy Act include the right to be informed about the mechanism of automated processing (either entirely of or partially) of their personal data; and the right to be safeguarded against automated decision-making that has legal consequences for them. Moreover, the data controller/processor must retain records of automatic processing of personal data for one year following the end of the calendar year in which the operations occurred.

7.11 Are there other specific advertising practices that you wish to discuss?

No specific advertising practices.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

In the view of globalization, transferring personal data is inevitable part of business and other human activity. Therefore, international data flow is critical for today's global economic and social interaction. Notably, according to article 12 of Convention 108+, a party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another party.

Under the Privacy Act, cross-border data transfers are allowed to countries that provide an adequate protection of personal data. Members of the European Union and the EEA, as well as countries which have ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are amongst those which have an adequate level of protection of personal data. In addition, the Ukrainian government can adopt a list of countries that provide an adequate level of personal data protection. Moreover, countries whose capital market regulators have signed Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information are also considered to have an adequate level of protection of personal data.

Cross-border transfers of personal data are also allowed from Ukraine to countries which do not provide adequate protection of personal data, under one of the following bases:

- (a) an express consent to cross-border transfer;
- (b) the transfer is necessary to conclude or perform a transaction between the data controller and a third party for the benefit of the data subject;
- (c) the transfer is necessary to protect the vital interests of data subjects;
- (d) the transfer is necessary to protect the public interest, or to establish, secure and enforce legal demands; and
- (e) the controller of personal data has provided appropriate safeguards to ensure the confidentiality of the private and family life of the data subject.

It should be noted that personal data must not be transferred and shared outside Ukraine for any other purpose than that for which it was initially collected and processed.

Finally, considering the war with Russia, exchange of personal data with Russia is generally prohibited. This is also a matter of sanctions law.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Ukrainian law does not stipulate any specific requirements relating to cross-border data transfer agreements, other than that such agreements must be in writing. Moreover, in Ukraine, there are no model contractual clauses for data transfer agreements that are officially approved by Ombudsman. However, the American Chamber of Commerce in Ukraine has prepared the Template Data Transfer Agreement ('AmCham Template'). Whilst such templates are not binding, they can be used as a basis for drafting an agreement on cross-border data transfer. As there are no official model contractual clauses in Ukraine for cross-border data transfer agreements, most companies in Ukraine develop their agreements using either the AmCham Template or the standard (model) contractual clauses, which were adopted by the European Commission.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Ukraine? Are there minimum standards? Does this differ by sector or size of the entity?

There are currently no laws, requirements or standards that regulate data security in Ukraine. Accordingly, there is no single standard for data security, nor are there any requirements or rules for companies to implement any security standards for processing personal data.

That said, some companies are using international standards to secure data and implement them in their processes, eg, ISO 27001 Standards. In addition, they obtain ISO certifications and other international certifications in the field of information security.

Generally, data controller/data processor stipulates the list and the scope of measures aimed at safe processing of personal data with consideration of the legal requirements on processing personal data and informational security.

In accordance with new Law on Consumer Protection Rights, to prevent third parties' unauthorized access to the information-communication system of authentication of consumers that is carried out in e-commerce, the party may stipulate additional means of identification of consumers.

There are also some sectors in which data security standards are higher in the view of sensitivity of processed data—for example, in the field of payment services.

9.2 **How are personal data breaches regulated in Ukraine? What are the requirements for notification and response?**

Contrary to the GDPR, Ukrainian data protection laws do not provide any regulations for data breaches, nor any special requirements for responding to data breaches. Moreover, data controllers are not obliged to notify data subjects where a data breach occurs. However, some industries notify regulators (eg, telecoms companies).

Further, the Master Template (see question 5.1) contains general obligations on the data protection officer/department to inform the management of the data controller/data processor about any violation detected of the personal data protection legislation with the purpose of taking necessary measures. The Master Template also states that the data protection officer/department must properly document all facts relating to breaches of processing and protection of personal data.

10 **ENFORCEMENT AND PENALTIES**

10.1 **What penalties exist for non-compliance with privacy law?**

The Ombudsman, the courts and the police are responsible for enforcing the requirements of the Privacy Act, which can be enforced through administrative, criminal and civil actions. Therefore, it can lead to administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

The penalties in Ukraine for a violation of the Privacy Act are quite low. Practically, the worst-case scenario is an administrative penalty, where the highest fine can be the equivalent of about €800. There is a risk of criminal liability (with a worst-case scenario of either corrective labor for up to 2 years, probation supervision for a period of 3–5 years, restriction of liberty for 3–5 years, or imprisonment for the same term), but the enforcement practice to date has been minimal. To date, we are not aware of any decision in Ukraine, from the courts or other authority, outlining serious legal consequences for a company or individual based on a data protection violation. Moreover, the risk of being fined by the Ombudsman remains low.

10.2 Do consumers have a private right of action? What remedies are available to them?

Under Ukrainian legislation, individuals have a private right of action. Individuals in Ukraine can apply to the Ombudsman, police or the courts to seek legal protection from any illegal processing of their personal data. Moreover, under the Privacy Act, a data subject has the right to file a complaint to the Ombudsman or the court and use the available means of legal defense in case of violation of data privacy and personal data protection law. However, there is very little public awareness about data privacy laws or issues related to this matter. Therefore, very few claims have been brought to court by individuals regarding the infringement of data protection laws.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

According to its most recent annual report, in 2024, the Ombudsman received 857 complaints regarding potential violations of the right to personal data protection.

Based on the review of complaints received by the Ombudsman in 2024, proceedings were initiated, circumstances of violations were examined, response measures were taken, orders were issued to remedy identified violations, administrative offense reports were executed, and materials were referred to pre-trial investigation authorities for the initiation of criminal proceedings.

On December 19, 2024, Ukraine faced a major cyberattack on its state registries, reportedly the most severe to date, aimed at disrupting critical infrastructure. In response, the Ombudsman notified the Ministry of Justice, National Police, and Security Service, which have launched a pre-trial criminal investigation.

One illustration of an enforcement action is a case where, in May 2023, an applicant submitted a complaint to the Ombudsman, stating that he had received a Viber message offering financial aid, allegedly from an international organization. The message contained a link to a fraudulent website, where entering personal data resulted in the unauthorized withdrawal of funds from his bank card. Given the indications of a criminal offense, a formal request was sent to the National Police of Ukraine, which initiated criminal proceedings for fraud under the Criminal Code and launched a pre-trial investigation.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Ukraine?

There are no specific cultural features regarding privacy in Ukraine. Generally speaking, Ukrainian citizens are not very familiar with their rights regarding privacy and personal data. This lack of awareness extends to workplace practices, where employers are subject to general obligations to prevent discriminatory treatment, including direct or indirect restrictions on employees' rights and mobbing (psychological harassment in the workplace). Despite these legal safeguards, collecting data on equality, diversity, and inclusion remains uncommon, particularly regarding personal aspects such as gender identity, which may be classified as sensitive data under the Privacy Act. While societal attitudes are gradually evolving, Ukraine remains relatively conservative in certain respects.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

- (a) Ukraine is taking steps to align its personal data protection laws with the EU GDPR. The Ukrainian Parliament has resumed consideration of the Draft Law. The Draft Law is an amended and restated version of the current Privacy Act. This time, the Parliament seems to intend to adopt it within Ukraine’s overall EU integration efforts, and is, at the time of writing, at the second reading stage. The Draft Law, among other things, suggests significant increases in the penalties for violating personal data protection laws, almost to the level of GDPR fines: for individuals, ₴20 million (approx €461,000), and for legal entities, up to ₴150 million (approx €3.5 million) or 8% of the total annual turnover for the previous year.
- (b) Another draft law currently registered with the Parliament of Ukraine provides for the establishment of a new supervisory authority in personal data protection and defines the status, powers, principles of organization and procedure for the activities of this authority.
- (c) In addition to the GDPR, the Ukrainian Parliament has also prioritized the implementation of the e-Privacy Directive 2002/58/EC as a part of the process of integrating EU and Ukrainian legislation.
- (d) Although Ukraine has not obtained an adequacy decision from the European Commission pursuant to Article 45 of the GDPR, designating IT industry as a ‘specified sector within a third country’, this status is one that the Ukrainian IT association is actively seeking in order to improve the competitiveness of Ukraine’s IT services in the European market.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

- (a) The Ombudsman, despite limited enforcement in personal data matters, has provided valuable interpretative guidance, offering businesses clarity on several data-related issues. In particular:
 - (i) Master Template (see question 5.1);
 - (ii) Rules on the Ombudsman’s Supervisory Powers over Personal Data Compliance; and
 - (iii) Procedure for Notifying the Ombudsman of High-Risk Processing and Designated Data Protection Units or Officers.
- (b) The Law of Ukraine on Cloud Services (the ‘Cloud Services Law’) took effect on September 16, 2022. This Law introduced a complex regulatory framework for providing cloud and data center services for users in Ukraine. It has a strong focus on regulating the provision of such services to public authorities and operators of critical information infrastructure facilities, but its scope extends further, to B2B and B2C relations. Among other things, and, given the martial law in Ukraine, it is worth mentioning that, under the Cloud Services Law, service providers must not:
 - (i) use technical facilities located in territory where the public authorities of Ukraine temporarily do not exercise their powers (ie, territories temporarily affected by the war) and in the territory of any aggressor state (currently, only the Russian Federation);
 - (ii) use technical facilities owned by states or entities to which sanctions have been applied under the Law of Ukraine on Sanctions dated August 14, 2014.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Ukraine remains committed to modernizing its data protection framework amid geopolitical and regulatory pressures. Consequently, in response to martial law, the Ukrainian Government adopted Resolution No 910 of August 16, 2022, listing countries with adequate personal data protection for cross-border data transfers, published on the Unified State Web Portal of Electronic Services. Moreover, Ukraine has expanded its digital infrastructure with initiatives such as the Diia app, providing electronic personal documents and streamlined access to certain government services. While enhancing service delivery, these developments also raise important concerns regarding data privacy and risks of mass surveillance.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

For now, there are no major privacy-related challenges for companies doing business in Ukraine. The main challenges as of now are data protection rules for processing and transferring sensitive/extreme risks personal data both within and outside Ukraine.

The challenges will occur only after the GDPR and other international privacy standards have been implemented by the Ukrainian Parliament. For this reason, it is reasonable to monitor the legislative changes in Ukraine and to start preparing for the expected changes.

12.3 What do you envision the privacy landscape will look like in five years?

As Ukraine has achieved candidate status for EU membership (as of June 23, 2022), it is obliged to harmonize its legislation with the standards of EU legislation. Therefore, we assume that both the GDPR, the e-Privacy Directive, Convention 108+, and other privacy-related legislation will be adopted by the Ukrainian Government. Given Ukraine's ongoing legislative alignment with EU standards and the Council of Europe's opinion that the Draft Law provides a comprehensive, European-aligned data protection framework, adoption of GDPR-equivalent rules is likely within the next one or two years.

Based on these facts, the privacy landscape in Ukraine is going to start to change in the near future. In five years' time, the GDPR standards will have been implemented at State level, and thus businesses should have started to implement global privacy standards in their companies.

UNITED KINGDOM

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in the United Kingdom.

At the time of writing, the primary legislation regulating privacy in the United Kingdom is the Data Protection Act 2018 ('DPA') which sits alongside and supplements the UK General Data Protection Regulation ('UK GDPR'). The UK GDPR is the retained EU law version of the EU's General Data Protection Regulation. The DPA and UK GDPR together set out the main framework governing the processing of personal data in the United Kingdom.

In addition, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') implemented Directive 2002/58/EC (the 'ePrivacy Directive') in UK law (see the European Union chapter).

However, the above privacy laws are currently being reformed pursuant to the Data (Use and Access) Act ('DUA Act'), which has recently completed the legislative process in Parliament and received Royal Assent on June 19, 2025. The DUA Act includes a number of changes of interest to advertising practitioners, which are described further in this chapter. The majority of the DUA Act, including the changes described in this chapter, will be brought into force by commencement order (secondary legislation), likely over the next Parliamentary term. You can find more information on the DUA Act at <https://www.lewissilkin.com/insights/2025/06/25/what-you-need-to-know-about-the-data-use-and-access-act>.

In addition to the above, English law has also developed the tort of misuse of private information, which has enabled it to give effect to its obligations under the European Convention on Human Rights, although this chapter focuses on the UK GDPR and PECR.

1.2 What are the primary laws regulating privacy in the United Kingdom? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

As mentioned above, the primary laws regulating privacy in the United Kingdom have been the UK GDPR together with the DPA (and the PECR legislates electronic communications). As these largely mirror European Union laws, see the European Union chapter for further information.

The UK GDPR regulates all aspects of the processing of personal data (except for processing by law enforcement and intelligence agencies, which is regulated separately), from its collection, to its treatment, security, and storage, through to deletion. Accordingly, the UK GDPR applies to the use of personal data for advertising purposes, imposing obligations on advertisers and others in the advertising ecosystem, as well as affording certain rights to data subjects in relation to the use of their personal data for advertising and marketing purposes.

The DPA supplements the UK GDPR. For example, it:

- (a) stipulates additional conditions and safeguards for processing special category and criminal offense data in several scenarios (see question 3.2); and
- (b) adds exemptions to various parts of the UK GDPR, including in relation to data subjects' rights, and transparency obligations (these include where the information is subject to legal professional privilege, is necessary for establishing or defending legal rights, or for various 'public interest' reasons).

In addition, the PECR sit alongside the UK GDPR and provide for specific rules that apply in relation to electronic communications, including in respect of the use of ‘storage and access technologies’ (which for ease of reference, are referred to in this chapter as ‘cookies and similar technologies’) and the sending of direct marketing via electronic mail. These rules apply irrespective of whether personal data is processed for the purposes of the electronic communication, although more often than not personal data will be processed in relation to matters regulated by the PECR.

The DUA Act, once fully in force, will essentially combine these two regimes. Notably, it will not replace existing UK data privacy laws in their entirety but is instead drafted as an amendment to those existing laws, which will make it somewhat of a challenge for privacy practitioners to navigate. The hope is that a consolidated text might be released in due course.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

See the European Union chapter, which discusses self-regulatory standards set by the European Advertising Standards Alliance, IAB Europe, and the European Digital Advertising Alliance, which are widely adopted in the UK.

In addition, in the United Kingdom, the Direct Marketing Association (‘DMA’) publishes the DMA Code, which is mandatory for its members and sets standards of ethical conduct and best practice when carrying out direct marketing activities.

These self-regulatory standards complement, but do not supersede, UK privacy laws and are generally considered as best practice. Organizations that follow these standards are more likely to be able to demonstrate compliance with UK privacy laws, although there is ongoing debate around some of these frameworks and they are not a guarantee of compliance.

Note that the DUA Act introduces a new requirement for the Information Commissioner’s Office to encourage representative industry and sectoral bodies to draw up PECR codes of conduct. This is intended to promote best practice and provide greater clarity for organizations operating in the digital advertising ecosystem. In addition, we may well see the DMA pressing forward with a direct advertising certification scheme as anticipated by the UK GDPR to give advertisers even greater clarity.

1.4 How is privacy law enforced in the United Kingdom? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The Information Commissioner’s Office (‘ICO’) is the supervisory authority for the United Kingdom. The ICO is an independent public body and the Department for Science, Innovation and Technology is the ICO’s sponsoring department within Government. Note that, pursuant to the DUA Act, the ICO will be abolished, and the Information Commission (‘IC’) will be created. The aim is to bring the ICO into line with other UK regulators, making the IC a full corporation with board members.

The ICO is responsible for preparing statutory codes of practice on certain topics (for example, on ‘Age Appropriate Design’, which outlines how services should comply with the UK GDPR when using children’s data) as well as issuing practical, non-binding guidance on how to comply with the UK GDPR and the PECR. Of note to advertising and marketing practitioners, the ICO has in recent years issued updated guidance on direct marketing activities and the use of cookies and similar technologies.

The ICO enforces breaches of privacy legislation through investigatory and corrective powers, which include the power to impose fines for violations of the UK GDPR and PECR.

The IC will have the same powers as the ICO and, in addition, will have new powers, including a power to compel individuals to attend interviews with the IC through ‘interview notices’ and a power to require the production of documents or the preparation of a report.

It is also possible for individuals to bring claims for breach of the UK GDPR and the PECR in the United Kingdom’s civil courts—this is the mechanism by which individual data subjects can obtain financial redress. The prospect of representative litigation undertaken on behalf of a group of claimants remains a possibility, but the ability to bring such claims now seems more limited following the Supreme Court’s 2021 decision in *Lloyd v Google LLC*, which found that representative actions can be brought to establish liability for breaches of data protection legislation, but damages generally need to be dealt with by way of an individual assessment, with data subjects needing to prove that they have suffered damage as a result of the breach. Such claims are of particular relevance to controllers that process the personal data of large numbers of data subjects.

You can find more information on ICO’s enforcement action at <https://ico.org.uk/action-weve-taken/enforcement/>. If you would like to read about the ICO’s enforcement action under PECR, visit <https://www.lewissilkin.com/insights/2024/05/30/the-ico-fines-again-a-round-up-of-fines-issued-by-the-ico-in-2024>.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in the United Kingdom?

See the European Union chapter for information on the material scope of the EU GDPR, which applies equally to the UK GDPR (where references in the EU GDPR to ‘in the Union’ are replaced in the UK GDPR with references to ‘in the United Kingdom’).

2.2 Does privacy law in the United Kingdom apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes. See the European Union chapter for information on the territorial scope of the EU GDPR, which applies equally to the UK GDPR.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in the United Kingdom?

See the European Union chapter for the EU GDPR definition of ‘personal data’, which is also the applicable definition set out in the UK GDPR.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter for what data is considered ‘special category’ under the EU GDPR—this is mirrored in the UK GDPR, albeit the United Kingdom opted for a lower age for children to give their consent in relation to information society services: 13 years.

Note that ‘special category data’ includes not only personal data that specifies relevant details, but also personal data revealing or concerning these details. In some cases, information may be classified as

special category data because it is possible to infer or guess details about an individual that fall within a special category. However, the ICO has recently (seemingly in a departure from the position taken in the European Union) clarified in its guidance that whether data counts as special category data depends on whether the processing intends to make an inference linked to a special category, or whether there is an intention to treat someone differently on the basis of inferred information. Accordingly, the intention of the processing organization is a material factor to consider.

Also note that the DPA imposes additional conditions and safeguards when processing special category and criminal offense data. These include, but are not limited to, where the processing is necessary for the purposes of:

- (a) performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment;
- (b) health or social care purposes;
- (c) the administration of justice;
- (d) the prevention or detection of unlawful acts; or
- (e) certain protective functions, including protecting members of the public against dishonesty, malpractice, unfitness or incompetence, or mismanagement (these provisions are used by regulatory bodies—for example those regulating the professions—to investigate fitness to practice).

Do note that the DUA Act provides the Secretary of State with the power to expand the current scope of special category data without needing to formally amend existing legislation. Therefore, it is likely that in due course we may see this definition expand to include other types of personal data, the misuse of which is likely to cause significant harm, including children's data, data of vulnerable individuals and perhaps even financial data.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

It should be noted that there seems a very high bar as to whether data is truly anonymized (ie, where it is no longer identifiable), and often organizations confuse the closely related concepts of anonymization and pseudonymization. Further, it does seem that the ICO and the European Union take slightly different views on anonymization, particularly as to whether the same data can be anonymous in one person's hands but could then constitute personal data in another (colloquially known as the 'whose hands' test), with the ICO considering this a possibility and the European Union rejecting the idea.

On March 28, 2025, the ICO went a step further than its EU counterparts and published Anonymization guidance, aimed at helping organizations to understand anonymization (and pseudonymization) techniques, and setting out how these techniques impact data protection obligations and responsibilities. In this guidance the ICO confirmed that there are two key factors to consider when determining whether data is considered personal or not. These are singling out (ie, being able to isolate a person from a set of records) and linkability (ie, being able to combine the data with other records across a single system or multiple systems). Ultimately, in the ICO's view, the question on whether data is anonymous will turn on whether there are means 'reasonably likely' to be used by the organization or someone who might gain access to an organizations' data to identify someone, taking into account objective factors such as the cost and time required and available technology. Interestingly, with respect to the 'whose hands' test, the ICO maintains its position that the same data can be personal in

the hands of one person and anonymous in the hands of another, but acknowledges that this is unlikely to be the case in a joint controllers or controller/processor relationship. This is interesting to note in an advertising context where joint controller and controller/processor relationships are commonplace.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter; the key obligations set out in the EU GDPR are also set out in the UK GDPR.

In addition, the ICO has produced its own guidance on many of these obligations (for example, on transparency requirements; how to maintain a record of processing activities; when to conduct a data protection impact assessment ('DPIA'); how to deal with personal data breaches; and compliance in relation to direct marketing and the use of cookies). This guidance is broadly in line with the key principles of EU guidance, but does provide additional insight into what controllers should do in practice to comply with the UK GDPR and PECR. For example, in relation to carrying out marketing via social media, the ICO encourages organizations to be 'upfront' (and to not overly rely on information buried in privacy notices) by using 'just in time notices' or taking a layered approach to transparency, makes clear that organizations should offer individuals control, and says that advertisers should take care to ensure that the social platform has provided all necessary information to individuals.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter; the roles set out in the EU GDPR are also set out in the UK GDPR.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Yes. See the European Union chapter, which applies equally for the purposes of UK privacy laws.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter, which applies equally for the purposes of the UK GDPR.

See also question 7.9 in respect of the processing of children's personal data when providing online products or services that are likely to be accessed by children.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter; the privacy rights set out in the EU GDPR are also set out in the UK GDPR.

It is worth noting that data subject access rights in the UK GDPR are commonly exercised in the United Kingdom, and the right to obtain copies of personal data is taken seriously by the ICO.

In particular, data subject access requests are commonly used to try to obtain documents as a precursor to litigation (particularly in employment-related disputes), or as a pressure tactic in the case of pre-action disputes. However, controllers should be wary about ignoring such requests. Case law is clear that these purposes do not render the request invalid.

The DUA Act introduces several notable changes to this right. When a controller requests clarification on the scope of a subject access request, the response deadline will be paused (the ‘clock is stopped’) until the individual replies, and controllers are only required to conduct a ‘reasonable and proportionate’ search—this is a more practical approach than that cited in the European Data Protection Board’s guidance on right of access, which does not generally allow for proportionality limits.

The DUA Act also creates a new ‘right to complain’ to controllers about UK GDPR compliance, which may mean privacy notices and internal processes will need updating to reflect this.

Rules around the data subject’s right to not be subject to automated decision-making are also clarified and relaxed under the DUA Act—see question 7.10.

5.3 **Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?**

The UK GDPR does not contain consent or opt-out requirements for specific circumstances. However, in practice, the ICO considers that many processing activities for advertising purposes either require consent (especially where processing activities are intrusive or would not be within the reasonable expectations of individuals) or should only be carried out in reliance on legitimate interest if an opt-out is provided. So-called ‘custom audience advertising’ (where advertiser first party data is shared with, and matched with the data of, advertising platforms to display ads to an advertiser’s customers (their ‘audience’)) is one such example, and there has been considerable debate about whether consent is required for such activity.

The PECR contain specific consent and opt-out requirements for certain activities. In particular:

- (a) Consent is generally required to send electronic mail (including email and SMS) for a direct marketing purpose to persons acting in their individual capacity. (see also question 7.1).
- (b) Consent is also required to use cookies and similar technologies that store information, or access information stored, on the devices of individuals for non-essential purposes. In most scenarios, the use of such technologies for advertising purposes (including for relatively unintrusive purposes, such as ad measurement) is not considered to be essential, and therefore consent will be required.

Note, the DUA Act proposes some key reforms in respect of the PECR’s requirements in relation to cookies and similar technologies. In particular, the Bill proposes to extend the obligation so that it applies to any person who ‘instigates’ the use of cookies and similar technologies, meaning that the technology companies that operate the technologies, as well as the website operators themselves, may be liable for non-compliance. In addition, the Bill proposes some new exemptions from consent requirements where technologies are used for certain purposes (such as certain analytics purposes (although data subjects are still permitted to opt out of the basic analytics technologies)), but the proposals do not go so far as

to introduce any advertising specific exemptions, even for relatively unintrusive purposes. However, the DUA Act grants the Secretary of State the power to amend the list of exemptions by making changes through secondary legislation (statutory instruments).

Where consent is required, the consent must be freely given, specific, informed, and unambiguous, typically obtained through a clear affirmative action (such as ticking a box or clicking an ‘accept’ button).

For cookies and similar technologies used for an advertising purpose, the ICO has recently required organizations to implement a ‘reject all’ button on their online service’s consent mechanism, and is clear that consent must be obtained before any non-essential cookies are set.

Where consent is required under the PECR, individuals must be able to withdraw their consent or opt out at any time, and this process must be as easy as giving consent. In practical terms this means that, for cookies and similar technologies, organizations must provide individuals with a means of changing their cookie preferences through the use of a ‘cookie settings’ button implemented in the footer of a website or in the settings of other types of online services. For electronic marketing, organizations are encouraged to provide individuals an easy way to amend their marketing preferences by way of a preference center, and unsubscribe links must be included in all electronic mail marketing communications.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter, which applies equally for the purposes of UK privacy laws. In addition, note that it is common practice for data protection agreements to be in place regardless of the role (ie, processor, controller or joint controller) of the vendor or third party that processes personal data.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for privacy law obligations, which are mirrored in the UK data protection regime.

In addition, the PECR sit alongside those privacy law obligations and provide for specific rules that apply in relation to electronic communications.

Amongst other things, the PECR prohibit persons from sending (or instigating another person to send) unsolicited communications to individual subscribers via electronic mail, where the communications are made for the purpose of direct marketing. The prohibition applies unless the organization:

- (a) has obtained consent (which must satisfy the conditions for consent prescribed by the UK GDPR) from the recipient; or
- (b) can rely on what is known colloquially as the ‘soft opt-in’ or ‘existing customer’ exemption. This exemption will apply where the following conditions (which are narrowly interpreted) are satisfied:
 - (i) the organisation carrying out the marketing obtained the recipient’s contact details ‘in the course of the sale or negotiations for the sale of a product of service to that recipient’;
 - (ii) the marketing is in respect of the organization’s ‘similar products and services only’; and
 - (iii) a ‘simple means of refusing’ the marketing (ie an opt-out) is offered at the point of collecting the personal data and in each subsequent marketing communication.

The communication itself does not need to contain any ‘marketing material’. The prohibition will apply where the purpose of the communication is to undertake direct marketing. As such, an organization will breach the PECR if it sends an electronic mail to a recipient which asks the recipient to confirm whether or not they want to receive direct marketing communications from the organization.

The words ‘electronic mail’ are interpreted broadly by the ICO, although the limits of these words have not been fully tested in English courts. These words clearly include traditional emails and text messages. However, the ICO has expressed the view (in its direct marketing code of practice—still in draft at the time of writing) that ‘electronic mail’ includes other types of communications that can be stored electronically, including push notifications and private messages sent to a social media inbox.

The prohibition only concerns ‘individual subscribers’ and not ‘corporate subscribers’. Broadly, this is understood to mean that B2B communications are not caught by the prohibition; but care needs to be taken, because some businesses (in particular, sole traders and some partnerships) are treated as individual subscribers.

Finally, the PECR also regulate other forms of communications, including live and automated telephone calls and faxes, although these forms of communications are outside the scope of this chapter.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter, which applies equally for the purposes of UK privacy laws. By way of clarification, where cookies and similar technologies store information or access information stored on user devices for non-essential purposes, the PECR require user consent (which must satisfy the conditions for consent prescribed by the UK GDPR) to be obtained. This is a separate requirement to having a lawful basis for any processing of personal data by such technologies (see also question 5.3). Do note that, in its latest cookie guidance, the ICO has deliberately moved away from referring to ‘cookies and similar technologies’ and instead refers more broadly to ‘storage and access technologies’, to clarify that any technology that either stores information on a user’s device or accesses information will be caught. The ICO specifically cites, in a non-exhaustive list, that cookies, tracking pixels, link decoration and navigational tracking, web storage, fingerprinting techniques, scripts, and tags are examples of such technologies.

7.3 **How are loyalty programs and promotions regulated under privacy law?**

See the European Union chapter, which applies equally for the purposes of UK privacy laws and the PECR.

In addition, the ICO has recently issued guidance about compliance with direct marketing consent requirements (see questions 5.3 and 7.1) in the context of loyalty schemes. The ICO says that organizations may be able to rely on the soft opt-in exemption to send marketing communications to persons that sign-up to a loyalty scheme, but it also emphasizes the importance of ensuring that customers understand what messages they will receive.

7.4 **How is social media and influencer marketing regulated under privacy law?**

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

In addition, given the propensity for social media to be used for direct targeted or behavioral advertising to individuals, including by use of social media operated tracking technologies (such as ‘plug-ins’), see questions 7.2 and 7.5.

7.5 **How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?**

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

Targeted advertising activities have previously been an area of focus for the ICO. In June 2019, the ICO issued a report setting out its concerns about the use of personal data where ads are delivered through ‘real time bidding’ (ie, an instantaneous and automated process for auctioning online ad space) and described the industry as ‘immature in its understanding of data protection requirements’. If you would like to read more about this report, visit <https://www.lewissilkin.com/en/news/ico-update-report-into-ad-tech-and-rtb>.

The ICO also issued an Opinion in 2021 where it built on the concerns set out in its 2019 report by setting out privacy standards that the ICO expects adtech vendors to meet when developing new products. If you would like to read more about this Opinion, visit <https://www.lewissilkin.com/en/insights/ico-opinion-data-protection-and-privacy-expectations-for-online-advertising-proposals>.

The ICO has also recently issued new guidance on the use of cookies and similar technologies, which includes a section on online advertising. In this guidance, the ICO makes clear that the use of cookies and similar technologies for online advertising purposes requires consent, and that this applies for the technical processes involved in delivering ads as well as associated tracking and profiling, and ad measurement, activities.

In its 2025 Online Tracking Strategy, the ICO has placed renewed emphasis on encouraging the adoption of contextual advertising and the use of privacy enhancing technologies to reduce the reliance on personal data in advertising. The ICO has signaled that it expects organizations to move towards less intrusive forms of advertising and is also working with government to explore changes to the law that would further support privacy-preserving advertising models.

7.6 **How are digital identity resolution and clean room technologies regulated under privacy law?**

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

The ICO have made clear that UK privacy law requirements apply both to data brokers themselves as well as the organizations using their services. In particular, organizations that use the services of data brokers should carry out due diligence to (amongst other matters) ensure that adequate transparency has been provided to data subjects (about the collection, sharing and use of their personal data), and that there is a lawful basis for the sharing and subsequent processing of the personal data.

In October 2020 the ICO took enforcement action against the credit reference agency Experian Limited, and published a report on its investigation into the direct marketing data broking sector. If you would like to read more about this, see <https://www.lewissilkin.com/en/insights/the-ico-takes-action-in-the-offline-data-broking-sector>. In addition, the ICO has also published specific advice for organizations using marketing services of data brokers: <https://ico.org.uk/for-organizations/direct-marketing-and-privacy-and-electronic-communications/organizations-using-marketing-services-of-data-brokers/>.

Therefore, while data broking activities are not specifically regulated from a data protection perspective, they are a specific form of activity that the ICO is concerned about.

7.9 How is advertising to children and minors regulated under privacy law?

UK privacy laws do not contain any specific requirements for advertising to children and minors. However, the ICO have made clear that if children's personal data is used for marketing purposes, a DPIA must be carried out to establish whether the processing will result in a high risk to the rights and freedoms of data subjects—because the ICO considers that targeting marketing at children is a circumstance which is likely to result in such a risk.

In addition, to ensure that processing activities are fair, lawful and transparent (and are otherwise compliant with the UK GDPR), organizations need to take care to ensure that they explain how they are using personal data in a way that children can understand, and should not exploit any lack of understanding or vulnerability.

In addition, where offering online services that are likely to be accessed by children, the ICO's Age Appropriate Design Code (also known colloquially as the 'Children's Code') mandates clear, age-appropriate privacy notices, and high default privacy settings. Any features relying on profiling—such as those used for behavioral advertising—must be switched off by default unless there is a compelling, child-focused justification. In practice, this means non-essential, commercially driven profiling (including behavioral advertising via cookies) must remain off unless and until valid, opt-in consent is obtained.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter, which applies equally for the purposes of UK privacy laws. Note, at present there is no separate legislation in the United Kingdom specifically regulating the use of artificial intelligence.

It should also be noted that rules around automated decision making ('ADM') will be significantly relaxed under the DUA Act, provided no special category data is processed in connection with ADM. This means it is likely that use of ADM in respect of significant decisions in an advertising context (assuming no special category data is involved) will go from prohibited to authorized subject to safeguards. These safeguards include informing individuals about significant decisions made solely by automated means, offering the right to contest or make representations regarding the decision, and enabling individuals to request human intervention.

7.11 Are there other specific advertising practices that you wish to discuss?

None in particular.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter, which applies equally for the purposes of UK privacy laws except that, with effect from March 21, 2022, the UK government has introduced, for processing that falls within the scope of the UK GDPR, two specific UK approved transfer mechanisms for the transfer of personal data to organizations in non-adequate countries. The two mechanisms are the UK Addendum to the EU Standard Contractual Clauses ('SCCs') and the UK International Transfer Agreement.

The two approved mechanisms are broadly the same in effect (despite having a different look and feel), although the UK Addendum is the preferred transfer mechanism for legitimizing the transfer of personal data outside of the United Kingdom to a non-adequate country.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter, which applies equally for the purposes of UK privacy laws.

In addition, as a result of Brexit, the United Kingdom is a 'third country' insofar as the European Union is concerned. Consequently, transfers of personal data from the European Economic Area ('EEA') to the United Kingdom are treated the same as transfers of personal data from the European Union to other non-EU territories. The United Kingdom has received an adequacy decision from the European Commission, and therefore such transfers do not require appropriate safeguards (eg, SCCs) to be implemented in respect of such transfer.

However, for the first time, the European Commission has limited the United Kingdom's adequacy to a four-year period, after which the adequacy decision will be reassessed, and renewed if the United Kingdom continues to ensure an adequate level of data protection. The adequacy decision was originally set to expire on June 27, 2025. However, at the time of writing, this has now been extended to December 27, 2025, to provide additional time for the United Kingdom to finalize the DUA Act (which was finalized on June 19, 2025) and for the European Commission to assess whether the United Kingdom's evolving data protection regime continues to meet the required adequacy standards.

Transfers of personal data in the opposite direction—ie, from the United Kingdom to the EEA—are not at present restricted and no additional safeguards are necessary.

Finally, at the time of writing, jurisdictions that are recognized by the European Commission as offering an adequate level of protection are also recognized by the United Kingdom as offering an adequate level of protection. However, in the future it is possible that the United Kingdom may recognize other jurisdictions as being adequate.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in the United Kingdom? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter; the security obligations set out in the EU GDPR are also set out in the UK GDPR. Note, the UK government plans to introduce a Cyber Security and Resilience Bill in 2025 to introduce new laws to enhance cyber defenses and protect essential public services. Existing regulations cover transport, energy, drinking water, health, and digital infrastructure sectors. They also govern digital services, such as online marketplaces, search engines, and cloud computing. This Bill will expand the scope of those regulations so that they will apply to more digital services and supply chains, enhance regulatory powers, and increase incident reporting requirements to improve the government's understanding of cyber threats.

9.2 How are personal data breaches regulated in the United Kingdom? What are the requirements for notification and response?

See the European Union chapter; the data breach obligations set out in the EU GDPR are also set out in the UK GDPR.

In addition, the ICO has produced additional guidance on data breach requirements, including when a breach may be notifiable, when individuals should be informed and what to do where the data controller has only partial information about the breach available.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter, which applies equally for the purposes of UK privacy laws, except that under the UK GDPR the maximum fine that an organization can receive is £8.7m (for less severe violations) or £17.5m (for serious violations).

Note, currently the maximum fine for a breach of the PECR is £500,000, although the DUA Act will increase this to be in line with the UK GDPR, ie, the maximum possible fine for a breach of the PECR will be £17.5 million or 4% of global annual turnover, whichever is higher.

As is the case in certain EU Member States, UK privacy laws create a number of criminal offences, including unlawfully obtaining personal data and re-identifying de-identified personal data. Moreover, the Computer Misuse Act 1990 criminalizes unauthorized access to computer systems and data.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter, which applies equally for the purposes of UK privacy laws, except that the ability to bring representative litigation in the United Kingdom now seems more limited following the Supreme Court's 2021 decision in *Lloyd v Google LLC* (as to which see question 1.4).

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In recent years the ICO's focus has been to ensure compliance with cookies consent requirements (see question 5.3) when such technologies are used for an online advertising purposes.

In particular, in late 2023, the ICO wrote to 53 of the UK's top 100 websites where it considered that they did not give users fair choices over whether or not to be tracked for personalised advertising purposes. In particular, the ICO required organizations to make it just as easy for users to 'Reject All' advertising technologies as it is to accept them (<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/commissioner-warns-uk-s-top-websites-to-make-cookie-changes/>).

In its 2025 Online Tracking Strategy, the ICO signalled its intent to continue this work by expanding its focus to the top 1,000 websites in the United Kingdom, as well as apps and connected TVs, aiming to ensure users have real choice and control over tracking. The ICO is also developing an AI solution to help identify non-compliant cookie banners at scale, signalling a more proactive and tech-driven approach.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in the United Kingdom?

None.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Companies should carefully monitor the work that the ICO is carrying out pursuant to its online tracking strategy. In early 2025, the ICO set out its priorities for the industry, stating that it expects organizations deploying advertising technologies to provide meaningful control to users—to help them choose what to share, with whom, and the purposes for which it can be used—with the ultimate aim of safeguarding and empowering people. As part of this strategy, the ICO is already taking action against the most popular websites in the United Kingdom (see question 10.3). However, the ICO have also said that they intend to ensure that people have meaningful control over tracking or personalised advertising on apps and connected TVs—therefore companies should look out for further movement from the ICO in this space.

Companies should also carefully consider whether their advertising and marketing practices—including their use of cookies and similar technologies for advertising purposes—are likely to be targeted to vulnerable persons. In a recent landmark decision (*RTM v Bonne Terre Ltd & Hestview Ltd*) the High Court found that a gambling platform had not obtained effective consent from the claimant—a reformed problem gambler—for the use of cookies or the sending of direct marketing. In the case, the Judge found that the claimant's ability to provide consent (to a UK GDPR standard) was impaired. Whilst the facts of the case concerned a gambling operator, the case has potential application to marketers who, due to the nature of their services, may target other categories of vulnerable persons, such as children or those who suffer from other addictions or health conditions. We anticipate further intervention from regulators or courts to protect such vulnerable persons.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

None in particular.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

As mentioned in question 10.3, in recent years the ICO has taken a more active approach to enforcing the PECR consent requirements in relation to the use of cookies and other similar technologies for advertising purposes. This action has spurred the emergence of so-called ‘consent or pay’ models by major publishers in the United Kingdom—where users of publisher websites are presented with a binary choice between consenting to personalized advertising or paying a subscription fee.

The ICO has opined that consent or pay models can be compliant with data protection law, provided they offer users a genuine choice and are implemented in a fair and transparent manner. Factors such as the appropriateness of the fee, the equivalence of the paid and ad-funded services, and the avoidance of power imbalances will be critical in determining compliance.

At the time of writing, such models have not been generally adopted by social media platforms (even those that have adopted such a model in the European Union, such as Meta), although, as a result of challenges being brought by privacy activists in the United Kingdom as well as other pressures (see question 12.2), we anticipate that social media platforms may introduce such models in the United Kingdom.

The DUA Act will also bring changes to the United Kingdom’s privacy landscape when in force, including increased fines for breaches of the PECR (see question 10.1) and furthering the scope of the PECR’s consent requirements for cookies and similar technologies to those that ‘instigate’ the use of such technologies (see question 5.3). It remains to be seen whether these changes will mark a sharp increase in the volume and amount of monetary penalties issued by the ICO for breach of the PECR.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Despite the UK GDPR being in effect for over seven years, there remains considerable uncertainty in certain areas. Notably, there remains considerable debate about the extent to which consent is required—or whether legitimate interests can be relied on—for certain advertising and marketing activities, such as for ‘custom audience’ advertising purposes (where advertiser first party data is shared with, and matched with the data of, advertising platforms to display ads to an advertiser’s customers (their ‘audience’)) and for other marketing related purposes, including for profiling and personalization.

This uncertainty is compounded by diverging regulatory change in the European Union, including decisions of the Court of Justice of the European Union and the Direct Markets Act, which require consent to be obtained, especially if advertising on large online platforms. Organizations looking for a ‘one-size-fits-all’ approach may find themselves taking decisions which are, from a purely-UK perspective, relatively conservative.

However, despite the position in the United Kingdom being less clear cut, we anticipate further movement in the United Kingdom towards consent-based models. This is likely to be the case due to increased regulatory action from the ICO against organizations that do not obtain effective consent for the use of cookies and similar technologies (with the current ICO focus being on websites, but with apps and other platforms such as connected TV also being on the agenda) and privacy activists bringing various challenges, including objecting (pursuant to the UK GDPR) to the use of their personal data for direct marketing purposes (see, for example, *Tanya O'Carroll vs Meta Platforms Ireland Limited*).

Additionally, whilst much of the hype surrounding international transfers has calmed since culminating in 2023 with the Irish Data Protection Authority's €1.2billion fine against Meta Platforms Ireland Limited, compliance with international transfer requirements (including transfer risk assessments) remains a compliance burden for many organizations. Uncertainty surrounding the United Kingdom's adequacy status with the European Union, as well as the potential for divergence in regulatory approaches, means that companies operating across borders must remain vigilant and adaptable to ongoing changes.

12.3 What do you envision the privacy landscape will look like in five years?

The DPA mandates the ICO to publish a statutory code of practice on direct marketing. The ICO issued a draft of such code for consultation in 2020. However, due to proposed changes to UK data protection law proposed by previous governments, followed by the introduction of the DUA Act by the current government, the ICO paused its efforts to finalize the code and instead issued updated guidance in 2020. Now that the DUA Act has passed its legislative process, the ICO is expected to reintroduce its direct marketing code. Amongst other matters, we expect clarity around the lawful basis that organizations may rely on to carry out 'custom audience' advertising and to process personal data for other direct marketing purposes, including for profiling and personalization activities (see question 12.2).

We envision further regulation or increased regulatory intervention in respect of the use of personal data for artificial intelligence ('AI') related purposes, including for training AI models, with a focus on fairness, discrimination, bias, and other individual harms.

As noted above, we also anticipate that more organizations, including social media platforms, will adopt so-called 'consent or pay' models. With that, we anticipate challenges to such models being brought by privacy activists who will challenge the validity of the consent obtained through such models. It remains to be seen whether some—in particular large online—platforms will be required to offer additional choice to users (such as a free but 'less personalized' version of the applicable service, similar to the approach taken by Meta in the European Union).

Companies that do not, or cannot, adopt such models due to the nature of their business are likely to need, in any event, to make changes to the way in which they obtain consent for cookies and other similar technologies, in light of enhanced ICO enforcement (see question 10.3) and the potential for increased fines for a breach of the PECR (see question 10.1), which will increase the risk associated with non-compliance.

Finally, as noted in question 11.2, we also expect more regulatory or court intervention in relation to the use of personal data of vulnerable persons, including children and individuals with health problems that may impair their ability to exercise effective judgment, for advertising purposes.



UNITED STATES OF AMERICA



1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in the United States.

US privacy is governed by a patchwork of federal, state, local, and sector-specific laws and self-regulation rather than a single comprehensive framework. This patchwork creates a fragmented compliance environment, especially for businesses engaged in advertising.

1.2 What are the primary laws regulating privacy in the United States? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

- (1) **Federal law:** There is no comprehensive federal privacy law. Instead, the Federal Trade Commission Act ('FTC Act') is the cornerstone of federal privacy regulation. While not explicitly a privacy statute, it prohibits unfair or deceptive acts or practices in commerce and is the primary tool for addressing privacy and data practices, particularly those involving advertising.
- (2) **State privacy law:** 19 states have enacted comprehensive privacy laws. While these laws share common features, they generally fall into two major models:
 - (a) **California model:** The California Consumer Privacy Act ('CCPA') was the first state comprehensive privacy law enacted and remains distinct from other state privacy laws in substance and enforcement. The CCPA applies to for-profit entities ('businesses') that meet certain thresholds and process the personal data of California residents ('consumers'). It grants consumers rights to access, correct, and delete their personal data, and to opt out of the sale or sharing of their personal data. Businesses must post detailed privacy disclosures, obtain opt-in consent before offering financial incentives tied to data use, execute contracts with service providers and third parties, maintain reasonable security measures, and provide privacy training to employees. The CCPA also includes implementing regulations with obligations around automated decision making, security audits, risk assessments, and more.
 - (b) **Consensus law model:** The Virginia Consumer Data Protection Act ('VCDPA') was the second state comprehensive privacy law enacted. All subsequent states have modeled their laws on the VCDPA, though with important differences in substance and scope. Consensus model laws apply to companies ('controllers') that meet certain thresholds and process the personal data of state residents ('consumers'). These laws generally grant consumers the rights to access, correct, and delete their personal data, and to opt out of the processing of personal data for purposes of targeted advertising, sales, and certain types of profiling. Controllers must post detailed privacy disclosures, obtain opt-in consent for processing sensitive data, maintain reasonable security measures, execute contracts with processors, and conduct data protection assessments for high-risk processing activities.
Some consensus model laws have unique requirements. For example, Maryland's privacy law imposes a strong data minimization requirement and purpose limitation standard. Several states include obligations around universal opt-out mechanisms and limitations on the use of dark patterns to obtain consent. As a result, while many states follow the consensus model, compliance strategies must account for meaningful variations in scope, enforcement authority, and technical obligations.

Of the 19 states with comprehensive privacy laws, 16 will be effective by the end of 2025: California, Virginia, Colorado, Connecticut, Utah, Iowa, Tennessee, Montana, Oregon, Texas, Delaware, Nebraska, New Hampshire, New Jersey, and Maryland. The three remaining take effect in 2026: Indiana, Kentucky, and Rhode Island.

In addition to comprehensive privacy laws, all 50 states have unfair or deceptive acts or practices ('UDAP') statutes that mirror the FTC Act and can be used to enforce privacy-related obligations. California also has several longstanding privacy laws that continue to apply to online services, including the California Online Privacy Protection Act ('CalOPPA') and Shine the Light, which governs certain types of data sharing for marketing purposes.

- (3) **Sectoral laws:** There are various sectoral laws at the federal, state, and local levels that apply to specific types of data or regulated industries or processes:
- (a) **Biometric privacy laws:** Many states and municipalities have enacted biometric privacy laws governing the processing of biometric information, such as facial recognition data, fingerprints, and voiceprints. The most notable is Illinois's Biometric Information Privacy Act ('BIPA'), which prohibits the collection or use of biometric identifiers without opt-in consent and provides a private right of action, making it a frequent source of class action litigation. Other laws. Many state privacy laws treat biometric data as sensitive personal data or a form of consumer health data, subject to heightened protections such as opt-in consent requirements and processing limitations.
 - (b) **Children and teens**
 - (i) The Children's Online Privacy Protection Act ('COPPA') prohibits the collection, use, or disclosure of personal data from children under 13 without verifiable parental consent. It directly impacts advertising models that involve audience targeting, personalization, or analytics on child-directed websites, apps, and online services.
 - (ii) Many state comprehensive privacy laws incorporate COPPA by reference and include additional protections for teens aged 13 to 15, such as requiring opt-in consent before selling or sharing teen personal data. For some states, restrictions on advertising apply to consumers ages 16 or even 17.
 - (iii) Some states have enacted age-appropriate design code laws or social media laws intended to increase protections for minors online. These laws have faced legal challenges, including in California, where litigation has questioned their constitutionality and scope.
 - (c) **Data brokers**
 - (i) The Fair Credit Reporting Act ('FCRA') is a federal law that regulates consumer reporting agencies and limits how companies may use credit, employment, insurance, or other eligibility-related data. It impacts data brokers and ad targeting platforms that rely on such information.
 - (ii) California, Vermont, Oregon, and Texas have enacted laws requiring data brokers to register annually with the state. California recently amended its data broker law through the Delete Act, which, starting in 2026, will require covered entities to process global opt-out requests submitted

through a centralized mechanism hosted by the California Privacy Protection Agency.

- (iii) Many state privacy laws include specific obligations around sales of personal data. For example, Nevada gives residents the right to opt-out of the sale of their covered information.

(d) **Education data**

- (i) The federal Family Educational Rights and Privacy Act ('FERPA') protects the privacy of student education records. It restricts how schools and edtech providers may use this data, including for advertising or other commercial purposes.
- (ii) Many states have passed laws governing the collection and processing of student data. California's Student Online Personal Information Protection Act ('SOPIPA') is among the most well-known and prohibits the use of student data for targeted advertising, building student profiles, or selling data.

(e) **Financial data**

- (i) The federal Gramm-Leach-Bliley Act ('GLBA') applies to financial institutions and governs the collection, use, and sharing of nonpublic personal information. It includes specific notice and opt-out requirements for sharing with non-affiliated third parties.
- (ii) State comprehensive privacy laws in California and New Jersey treat financial data as sensitive personal data, subject to heightened protections such as opt-in consent and processing limitations.
- (iii) Some states have enacted laws, such as the California Financial Information Privacy Act, that regulate financial data and financial institutions beyond or in addition to GLBA.

(f) **Electronic communications**

- (i) The federal Electronic Communications Privacy Act/Stored Communications Act restrict unauthorized access to and disclosure of the content of electronic communications and associated metadata. They have been cited in litigation involving tracking technologies, such as session replay tools, where companies allegedly intercept or store user communications without consent.
- (ii) State laws such as California's Invasion of Privacy Act ('CIPA') and similar statutes prohibit the interception of electronic communications without all-party consent and have become a key litigation tool in privacy cases involving tracking technologies.

(g) **Emails, texts, and calls**

- (i) The federal Controlling the Assault of Non-Solicited Pornography and Marketing Act ('CAN-SPAM') governs commercial email. It requires marketers to provide recipients with the ability to opt out of future communications, include clear sender identification, and avoid misleading subject lines or headers.
- (ii) The federal Telephone Consumer Protection Act ('TCPA') and Telemarketing and Consumer Fraud and Abuse Prevention Act regulate telemarketing practices, including phone calls and text messages. The

TCPA requires prior express written consent for autodialed or prerecorded marketing messages sent to mobile phones, significantly shaping outbound marketing strategies.

- (iii) Many states have enacted their own telemarketing laws with additional restrictions, Do Not Call registries, and penalties for non-compliance.

(h) **Health data**

- (i) The Health Insurance Portability and Accountability Act ('HIPAA') governs the use and disclosure of protected health information ('PHI') by covered entities (eg, healthcare providers, health plans, healthcare clearinghouses) and their business associates. It places strict limits on using PHI for marketing unless specific authorization is obtained and requirements to notify in the event of a breach, including potentially unauthorized disclosures through tracking technologies.
- (ii) Some states, including Washington and Nevada, have enacted specific consumer health data laws that apply to data outside the scope of HIPAA. Washington's My Health My Data Act is the most expansive, covering a broad range of health-related information—including inferred data—and requiring affirmative authorization to sell consumer health data, including for advertising. The law also restricts the collection of precise geolocation data near sensitive health locations, grants robust consumer rights, and includes a private right of action, creating significant compliance and litigation risk.
- (iii) Many comprehensive state privacy laws treat health data and precise geolocation data as sensitive personal data, subject to heightened protections such as opt-in consent requirements and processing limitations.
- (iv) Various state medical record laws and confidentiality statutes regulate the handling of health data, such as California's Confidentiality of Medical Information Act ('CMIA').

(i) **Security and breach notification laws**

- (i) Many state laws mandate specific administrative, technical, and physical safeguards for certain types of data, particularly in the context of consumer and employee information.
- (ii) All 50 states, the District of Columbia, and several US territories have breach notification laws requiring businesses to notify affected individuals, and often state regulators, when certain types of personal data are compromised.

(j) **Data transfers**

- (i) The DOJ's Data Security Program Rule ('DSP Rule'), sometimes referred to as the DOJ's Bulk Sensitive Data Rule restricts or prohibits transfers of bulk sensitive US data (eg, device identifiers or precise geolocation) to covered persons, even if the data is anonymized or de-identified. It applies to both direct and indirect disclosures, including through data brokerage and ad tech transactions, and may require strict security and contractual safeguards. Covered persons include any entity that is 50%

or more owned or controlled, directly or indirectly, by a person or government of a country of concern (eg, China, Russia, Iran).

- (ii) The Protecting Americans' Data from Foreign Adversaries Act prohibits any 'data broker'—an entity that sells or licenses personally identifiable sensitive data of US individuals—to transfer such data to a foreign adversary country or any entity controlled by a foreign adversary.

(k) **Video Viewership Data**

The federal Video Privacy Protection Act ('VPPA') prohibits the knowing disclosure of information identifying an individual's specific video viewing habits without their consent. In recent years, it has been used in lawsuits against media and streaming companies that embed tracking pixels or SDKs that share viewing history with third parties for advertising.

(l) **Artificial intelligence ('AI') and automated decision-making technologies ('ADMT')**

This is an emerging area of law, with states only recently beginning to regulate AI and ADMT. Most existing laws focus on algorithmic discrimination, use of AI in high-risk sectors (eg, education, healthcare, housing, employment, insurance), or consumer disclosures for AI chatbots. Currently, few requirements specifically apply to the advertising industry, but ongoing legal developments make this an area to watch.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulatory organizations like the Digital Advertising Alliance ('DAA'), National Advertising Initiative ('NAI'), and Interactive Advertising Bureau ('IAB') have helped shape privacy practices in advertising by promoting transparency, consumer choice, and accountability. Most self-regulatory programs play an increasingly complementary to expanding state-level privacy obligations, but their enforcement powers are limited and do not preempt state law.

1.4 How is privacy law enforced in the United States? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

(a) **Regulators**

- (i) The Federal Trade Commission ('FTC') is the main federal agency for consumer privacy enforcement. Using its FTC Act authority, it brings actions against companies engaging in unfair or deceptive data practices. The FTC has led enforcement in areas such as online tracking, data security, dark patterns, and children's privacy, setting de facto national common law standards through its settlements and guidance.
- (ii) State Attorneys General ('AG's') enforce both general consumer protection laws and state privacy laws. They can investigate and bring actions against companies for violating privacy obligations, such as failing to honor opt-out requests or misrepresenting data practices. California has been the most active enforcer to date, particularly through actions under the CCPA and broader unfair competition laws.
- (iii) The California Privacy Protection Agency ('CPPA') is the first and only state agency dedicated solely to privacy enforcement. Created under the CCPA, it has the authority to enforce the CCPA, issue regulations, conduct audits, and investigate potential violations. Though still relatively new, the CPPA has begun initiating enforcement

actions and is expected to play an increasingly active and influential role in shaping privacy compliance nationwide.

- (iv) Agencies such as the Department of Health and Human Services ('HHS') and the Department of Education enforce privacy laws within their respective domains, including HIPAA and FERPA.
- (b) **Self-regulatory bodies:** Self-regulation is not a source of binding legal authority. However, violations of self-regulatory codes may result in the loss of membership or referral to government enforcement bodies.
- (c) **Private right of action:** Although most US privacy laws do not grant individuals a right to sue, some statutes allow for private lawsuits, including CCPA (for certain data breaches), BIPA, TCPA, VPPA, and wiretapping laws. These laws often include statutory damages, meaning plaintiffs can recover fixed monetary amounts per violation without proving actual harm. As a result, companies may face class action lawsuits seeking damages totaling millions of dollars. This makes private enforcement a powerful and growing force in the US privacy landscape, despite the absence of a comprehensive federal law.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in the United States?

A company is subject to US privacy laws based on what personal data it collects, how it uses that data, where it operates, or whom it targets. The FTC Act applies broadly to companies engaged in commerce. State privacy laws apply when a company meets certain thresholds, such as processing a defined volume of personal data, generating revenue from data sales or advertising, or targeting residents of that state, regardless of physical presence. Sectoral federal laws, such as HIPAA, GLBA, and COPPA, apply when a company operates within a regulated industry or handles specific types of personal data.

2.2 Does privacy law in the United States apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, US privacy laws can apply to foreign companies, even without physical presence in the US, if they do business in the US, targets US residents, or collects personal data about them. State laws also have extraterritorial reach based on defined thresholds. Unlike the GDPR, US laws generally do not require foreign companies to appoint local representatives, but may still risk enforcement or litigation.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in the United States?

The definition of personal data (often called personal information) varies by law, but generally refers to information that identifies, relates to, describes, or reasonably could be linked to a particular individual or household. State privacy laws use broad definitions that include names, emails, device identifiers, IP addresses, geolocation data, and even inferences drawn from other information. Some laws, especially sectoral ones like HIPAA or GLBA, define personal data more narrowly, limiting it to data collected in specific contexts (eg, health or financial services).

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

Sensitive personal data generally includes categories such as precise geolocation (eg, latitude/longitude), biometric data, health data, financial account information, government identifiers, race or ethnicity, religious beliefs, sexual orientation, union membership, and the contents of private communications.

Comprehensive state privacy laws typically require opt-in consent before collecting or processing sensitive personal data, and impose additional obligations related to disclosure, purpose limitation, and security. The CCPA has a unique requirement that businesses must provide consumers with the ability to opt out of the use and disclosure of sensitive personal data for secondary purposes such as advertising or profiling. Some state and sector-specific laws go further, placing strict limits on the use of sensitive personal data for advertising, requiring separate affirmative consent, restricting downstream sharing, and mandating stringent data minimization requirements.

Children's and teen data also receive heightened protection. Under COPPA, companies must obtain verifiable parental consent before collecting personal information from children under 13 and are restricted from engaging in behavioral advertising. Some state privacy laws extend protections to teen data (typically, ages 13–15), requiring opt-in consent for targeted advertising and in some cases prohibiting it entirely based on age or data sensitivity.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Most US privacy laws exclude de-identified or anonymized data from their scope, provided the data cannot reasonably be linked to an individual and the company takes steps to prevent re-identification. For example, the CCPA excludes de-identified data only if the business maintains safeguards and publicly commits not to re-identify the information. In contrast, pseudonymized data, such as hashed emails or internal identifiers, remains covered if it can be re-linked to an individual. While definitions vary, in general, only fully de-identified data is exempt from legal obligations, not merely pseudonymized data.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Companies subject to US privacy law must comply with a range of obligations, which vary by law but generally include the following:

- (a) **Notice:** Companies must provide clear and conspicuous disclosures about their data practices, including what personal data is collected, how it is collected, the purposes for collection and use, to whom it is disclosed, details around use for advertising, and what rights consumers have.
- (b) **Consumer rights:** Companies must enable consumers to exercise privacy rights such as access, deletion, correction, and opt-out of the sale, sharing, or use of personal data for targeted advertising or profiling.
- (c) **Sensitive data:** Companies must treat sensitive data with enhanced protections, such as obtaining opt-in consent for collection or processing and providing opt-out options for secondary uses, such as advertising.

- (d) **Data minimization and purpose limitation:** Companies must limit collection to what is reasonably necessary and proportionate to the disclosed purposes.
- (e) **Contracts:** Companies must enter into contracts with service providers and other third parties that restrict how personal data can be used, retained, and disclosed.
- (f) **Security measures:** Companies must implement reasonable administrative, technical and physical safeguards to protect personal data from unauthorized access or misuse.
- (g) **Record-keeping and risk assessments:** In certain cases, companies must document data processing activities and conduct privacy risk assessments, especially for high-risk activities.

4.2 **Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?**

Yes, many US privacy laws assign companies roles based on their processing activities. Under consensus state privacy laws, companies are designated as controllers or processors: controllers determine the purposes and means of processing and are primarily responsible for compliance, while processors act on the controller's behalf under a binding contract. In some cases, two entities may be controllers, each responsible for its own use of the personal data.

The California model classifies companies as businesses, service providers, or third parties. A business may disclose personal information only to a service provider or third party, and each category carries distinct contractual requirements. If the recipient is a third party, the disclosing business must also offer opt-out rights to the consumer for that disclosure.

Sectoral laws like HIPAA use different terminology (eg, covered entities and business associates) but similarly require role-based compliance obligations and written agreements governing data handling.

4.3 **Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.**

US privacy law does not incorporate the concept of a lawful basis for processing personal data. Instead, it focuses on regulatory requirements, such as notice, purpose limitations, and contractual obligations, and may require consent for certain types of processing (eg, sensitive personal data or targeted advertising). However, consent in this context is a compliance requirement, not a legal basis.

California law includes the concept of a 'business purpose,' which is the closest analogue, limiting service providers to processing personal information only for specified business purposes on behalf of a business. If a recipient uses the data for its own purposes or for cross-context behavioral advertising, it is considered a third party, triggering additional compliance requirements.

5 **TRANSPARENCY AND CONSUMER RIGHTS**

5.1 **What information must companies include in their privacy notices when processing personal data for advertising purposes?**

When processing personal data for advertising purposes, companies must include clear, specific disclosures in their privacy notices, though requirements vary by state. Privacy notices should explain what personal data is collected (including via tracking technologies like cookies or pixels), how it is used for advertising, and whether it is shared or sold to third parties. They must also describe consumer rights, such as opting out of sales or targeted advertising, and how to exercise those rights,

often via a footer link like ‘Do Not Sell or Share My Personal Information.’ Some laws and self-regulatory frameworks (eg, the DAA or NAI codes) require specific language and opt-out mechanisms, and contracts with ad tech vendors may impose additional disclosure obligations.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have a range of privacy rights related to advertising, which vary by state and generally fall into three categories:

- (a) **Verifiable rights:** These rights require identity verification before fulfillment and typically include the rights to access, correct, delete, and obtain a portable copy of personal data. Some states provide a right to know about a company’s data practices, and a few go further—Minnesota and Oregon require companies to disclose the specific third parties to whom data was shared, while Delaware and Maryland require disclosure of the categories of third parties.
- (b) **Opt-out rights:** These rights do not require verification and are central in advertising contexts. Consumers may opt out of the sale, sharing, or processing of personal data for targeted advertising, and this opt-out must apply to both tracking technologies and CRM data (like email addresses). Some states require a prominent link in the footer (eg, ‘Do Not Sell or Share My Personal Information’) and mandate honoring opt-out preference signals such as Global Privacy Control (‘GPC’). Additional opt-outs in some states include the right to opt out of profiling or automated decision-making, and, in California, the right to limit the use and disclosure of sensitive personal information.
- (c) **Other rights:** These rights include the right to receive notice and opt in to financial incentives or loyalty programs, the right to appeal denials of rights requests, the right to use an authorized agent, the right to be free from discrimination for exercising privacy rights, and the right to withdraw consent.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

US privacy law generally requires companies to offer opt-out options when selling, sharing, or processing personal data for targeted advertising. For example, if a company uses pixels (eg, Meta’s) or shares data for matched audience advertising, it must give consumers an opt-out mechanism.

However, consent is required in certain circumstances:

- (a) **Sensitive data:** Most state privacy laws require opt-in consent to collect or use sensitive personal data, though definitions and requirements vary. The FTC has indicated that collecting sensitive data, like precise geolocation through ad networks, requires affirmative consent.
- (b) **Children and teens:** Under COPPA, companies must obtain verifiable parental consent before collecting personal information from children under 13. Certain state laws also require opt-in consent to sell or share teen data (ages 13–15), and some, like Maryland and Connecticut, extend protections to consumers under 18.
- (c) **Reasonable expectation test:** In states like California, companies must obtain opt-in consent for secondary uses of personal data that are inconsistent with a consumer’s reasonable expectations, based on the nature of the relationship, the type of data collected, and the specificity of disclosures.
- (d) **Text message marketing:** As discussed below, affirmative written consent is required before sending text messages.

- (e) **Video tracking:** The VPPA has been used to challenge the collection of video viewing history through tracking technologies (eg, pixels or SDKs) without prior, informed written consent, particularly when data is shared with third parties for advertising.
- (f) **Wiretapping litigation risk:** Recent lawsuits allege that the use of tracking technologies without consent violates wiretapping or electronic communications laws. In response, some companies have adopted consent management platforms to obtain opt-in consent before deploying trackers.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Companies that disclose personal data to vendors or third parties (eg, agencies, DSPs, SSPs, and data providers) in the advertising ecosystem must ensure these partners handle data lawfully through contractual safeguards and reasonable due diligence.

Most laws require written agreements with service providers or third parties that restrict unauthorized data use and mandate compliance with applicable privacy obligations. Under the CCPA, for example, businesses must ensure that service providers do not use personal information for cross-context behavioral advertising. The IAB's Multi-State Privacy Agreement offers a standardized self-regulatory framework to help ad tech participants meet contractual and disclosure requirements across jurisdictions, particularly when honoring opt-outs for targeted advertising.

State laws are increasingly holding companies liable for vendor misconduct if they fail to conduct reasonable diligence. CCPA regulations emphasize that inadequate vetting or oversight may expose companies to liability, even when a vendor's noncompliance is unintentional.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When disclosing personal data between a controller and processor, consensus model laws require companies to execute robust data processing addendums ('DPA'). These DPAs cover instructions for processing, the nature, purpose, and duration of processing, the type of personal data involved, the rights and obligations of both parties, a duty of confidentiality, requirements to return or delete data, recordkeeping, audit or assessment rights, and sub-processor restrictions.

The CCPA imposes unique contractual obligations. Contracts between a business and a service provider must include specific terms prohibiting the sale or sharing of personal information, limiting use to defined business purposes, and preventing the service provider from combining personal data with other information. If the contract is deficient, the recipient will be treated as a third party subject to consumer opt-out rights and other requirements. Contracts between a business and a third party also require specific terms, such as restricting use to specified purposes and granting the business rights to audit and remediate unauthorized data uses.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies are expected to proactively vet vendors to ensure compliance with privacy laws. This includes reviewing data practices, contractual commitments, and safeguards used.

Many state privacy laws require privacy impact assessments when engaging in activities that pose a heightened risk to consumers, such as targeted advertising, profiling, selling personal data, or processing sensitive data like children's, precise geolocation, or health information. These assessments must analyze the benefits and risks to consumer privacy, document mitigation measures, and be updated regularly, typically every two years or when processing practices materially change.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

US privacy law regulates direct marketing channels, such as email, text messages, or push notifications, through a combination of federal and state law, with distinct rules for each channel:

- (a) **Emails:** As noted in question 1.2, the CAN-SPAM Act is the primary federal law governing email marketing. It operates under an opt-out regime, meaning senders are not required to obtain prior consent but must provide recipients with a clear way to unsubscribe. CAN-SPAM includes requirements for truthful subject lines, sender identification, and a valid physical address. Enforcement has historically been limited due to the lack of a private right of action. While CAN-SPAM focuses on sending, other laws may apply to the collection and use of email addresses. For example, tracking pixels embedded in emails may trigger privacy obligations under state laws or sector-specific regulations. Similarly, if email addresses are collected and used for profiling, targeted advertising, or data sharing, businesses must consider applicable state privacy laws and ensure compliance with notice, consent, and purpose limitation requirements.
- (b) **Texts:** Text message marketing is primarily governed by the TCPA and the Telemarketing and Consumer Fraud and Abuse Prevention Act, along with various state-specific laws. The TCPA requires prior express written consent before sending marketing texts using an autodialer or prerecorded message. It also provides a private right of action, allowing individuals to sue for statutory damages of up to USD 500 per violation, or USD 1,500 per willful violation, without needing to show actual harm. Class action lawsuits under the TCPA are common and can result in substantial liability: if a company sends 10,000 unauthorized texts, it could face up to USD 15 million in statutory damages. Accordingly, companies should cautiously engage in phone or text-based marketing campaigns, ensuring they obtain compliant opt-in consent. As with email marketing, the TCPA focuses on the act of sending messages, but additional laws may apply to the collection and use of phone numbers.
- (c) **Push notifications:** No federal law specifically governs push notifications, but they are subject to general privacy and consumer protection laws, including state privacy statutes and the FTC Act. In most mobile ecosystems, users must provide consent to receive push notifications, and platforms like Apple and Google impose their own developer requirements for transparency and control.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

US privacy law regulates tracking technologies through the patchwork of federal, state, local, and sector-specific privacy laws and self-regulation discussed above. These rules are generally technology agnostic and apply to all tracking technologies, including cookies, pixels, SDKs, and others, regardless of form. Key compliance obligations include:

- (a) **Notice:** Companies must clearly disclose in their privacy policies the use of tracking technologies, including the categories of data collected, the purposes of use (eg, analytics, targeted advertising), the categories of recipients, and available consumer choices.
- (b) **Enhanced notice:** Some state laws and self-regulatory programs (eg, the DAA) require prominent, real-time notice at or before the time of collection. There is no standard for what enhanced notice means in practice. While US law does not expressly mandate cookie banners, many companies deploy them to align global compliance strategies and reduce litigation risk (eg, under wiretapping laws).
- (c) **Consumer choice:** Most comprehensive state privacy laws require companies to offer opt-outs of sales, shares, or targeted advertising that rely on tracking technologies. Some states, like California, mandate specific mechanisms, such as a 'Do Not Sell or Share My Personal Information' link and honoring GPC signals.
- (d) **Sensitive personal data:** The FTC and most states take the position that the collection of sensitive personal data through tracking technologies requires opt-in consent.
- (e) **Contracts:** Companies must ensure that third parties receiving personal data through tracking technologies are bound by contracts that include required restrictions.

Tracking technologies are a foundational part of the digital advertising ecosystem. They are used for a variety of purposes, including measurement, attribution, fraud prevention, and targeted advertising, and often support critical functions across the advertising supply chain. Evaluating legal risk requires assessing both how the tracking is used and how data is handled (eg, whether it is combined across contexts, repurposed, or used solely on behalf of a single party). Responsibility for compliance does not fall on a single entity; it is shared across the ecosystem, including publishers, advertisers, agencies, ad networks, DSPs, SSPs, and other ad tech intermediaries.

The use of tracking technologies in advertising is a major focus of regulatory enforcement and litigation. Legal risk often arises where companies fail to disclose tracking, configure tools in a way that impedes choice, create dark patterns, or process sensitive personal data without appropriate consent. Regulators and litigators are particularly focused on high-risk practices involving health data, children and teens, video viewing, precise geolocation, and technologies that are unexpected or opaque, such as session replay tools that monitor keystrokes and mouse movements or geolocation tracking in apps where such data collected would not be reasonably expected by the consumer.

Separately, platforms play an increasingly important role. For example, Apple's App Tracking Transparency framework requires iOS apps to obtain opt-in consent before tracking users.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions are subject to privacy law when they involve the collection of personal data. Some states, such as California and Colorado, impose additional requirements specifically addressing how these programs operate.

- (a) **California:** The CCPA requires businesses offering financial incentives, such as loyalty programs, to obtain opt-in consent before enrolling consumers. Consumers must be able to withdraw consent at any time. Businesses must also provide a 'Notice of Financial Incentive' at the point of registration, which must include:
 - (i) a summary of the incentive being offered;
 - (ii) the material terms of the program, including the categories of personal data collected and the value of that information;
 - (iii) instructions on how to withdraw from the program; and

- (iv) an explanation of how any price or service difference is reasonably related to the value of the consumer's personal data.
- (b) **Colorado:** Under the Colorado Privacy Act ('CPA'), businesses that offer 'Bona Fide Loyalty Programs' (programs that offer consumers better prices, rates, levels quality or selection of goods or services in exchange for participation) must ensure that participation is voluntary. While opt-in consent is not required for enrolment, businesses must provide notice about the categories of personal data collected, how it will be used, and who will receive it. If sensitive personal data is collected, opt-in consent is required. The CPA also requires a link to the business's privacy policy and, if applicable, an explanation of why deleting personal data would make it impossible to provide program benefits.

Several other states regulate loyalty programs but have less prescriptive requirements.

7.4 How is social media and influencer marketing regulated under privacy law?

Like other areas of digital marketing, social media advertising and influencer marketing are subject to privacy laws, but with added obligations around data sharing, targeted advertising, transparency, and protections for minors.

Social media advertising frequently relies on technologies, such as tracking pixels, SDKs, matched audience tools, and behavioral profiling, that trigger legal obligations. For example, if a brand places a social media platform's pixel on its own website, it must disclose that consumer data is being collected and shared with social media platforms. Depending on how the platform uses the data it receives, the brand may also need to offer consumers opt-outs from sales, shares, or targeted advertising. Brands and influencers are also responsible for complying with privacy laws when they collect data directly through social media platforms, such as where an influencer gathers email addresses through a link in their bio or runs sweepstakes or giveaways on social media. For a summary of privacy laws and obligations relating to tracking and advertising technologies, see questions 1.2 and 7.4.

Brands and influencers must also comply with the social media platform's own privacy rules and policies relating to use of social media tools or products, often going beyond legal minimums. These may include the mandatory use of branded content disclosures, limitations on how data collected through the platform can be used, and restrictions on uploading third-party data into custom audience tools. Failure to comply can result in account penalties, content removal, or de-platforming.

Because social media platforms are widely used by minors, they are subject to a range of legal obligations aimed at protecting children's and teens' data. For information on children's privacy, see question 7.9. Similarly, design code laws in California, Vermont, and other states require businesses to conduct risk assessments, estimate user age with reasonable certainty, and configure default privacy settings to offer maximal protection. These laws may also restrict profiling, behavioral nudges, and algorithmic targeting unless strictly necessary to deliver the core service. Unlike COPPA, these state laws may apply to a broader range of services, not just those directed at children, and therefore require more robust and proactive safeguards.

Several states have enacted laws aimed at curbing the potentially addictive and harmful aspects of social media platforms, especially for minors. These laws regulate the design and delivery of content feeds, notification timing, and access controls, often independent of whether personal data is being collected. For example, the New York Stop Addictive Feeds Exploitation (SAFE) for Kids Act prohibits platforms from delivering algorithmically curated content feeds to users under 18 without first verifying age or obtaining parental consent. It also restricts the use of overnight push notifications

directed at minors. California's Protecting Our Kids from Social Media Addiction Act imposes similar limitations, targeting feed design and encouraging platforms to deter compulsive usage. Utah's Social Media Regulation Act goes further, requiring platforms to obtain express parental consent for minors under 18 to create accounts, and mandating the implementation of time restrictions, parental monitoring tools, and other technical safeguards. These laws, while not privacy-specific, often interact with privacy obligations and should be considered in parallel. We note that several of these laws are subject to legal challenge or not yet in effect.

Additionally, federal requirements like the FTC's Endorsement Guides require influencers and brands to clearly disclose material connections, such as payment or free products, in a way that is conspicuous and easy to understand. The FTC also enforces truth-in-advertising standards, which apply to all commercial content, including filtered images, product placements, and AI-generated posts, and require that claims be truthful and not misleading. Certain industries, such as alcohol and health, are subject to additional rules enforced by agencies like the Alcohol and Tobacco Tax and Trade Bureau, Federal Drug Administration, or Federal Communications Commission.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Yes. Privacy law imposes stricter obligations on targeted advertising, which involves personal data processing across third-party services to personalize ads. The law typically requires clear disclosure, opt-out rights (or opt-in for sensitive data), and contractual restrictions on third party data use.

In contrast, contextual advertising is based on the content a user is viewing, not their identity or behavior. While it may involve tracking technologies for measurement, attribution, or fraud prevention, it generally does not trigger opt-out obligations under most laws.

The key distinction is not whether tracking is used, but how personal data is used, particularly whether it is shared or repurposed for broader profiling.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies raise unique privacy considerations because they involve linking, combining enriching, or analyzing personal data, such as emails, device IDs, or purchase history, from multiple sources across platforms or parties. Clean rooms are designed to enable data collaboration between parties without directly exposing raw datasets.

These technologies are often marketed as privacy-enhancing technologies or privacy-compliant by design. While providers may apply techniques like hashing or pseudonymization to reduce risk, these measures do not remove the activity from the scope of privacy law, particularly when data can be re-linked or used across contexts. Use of these technologies may constitute a sale, share, or profiling and can trigger obligations under state privacy laws, including notice, opt-out rights (or opt-in for sensitive data), and contractual restrictions on downstream use and sharing.

Regulators are increasingly scrutinizing these tools, especially when used for advertising, measurement, or audience targeting. Companies should carefully evaluate these tools on a case-by-case basis to ensure they meet applicable legal requirements.

7.7 How is location-based advertising regulated under privacy law?

Most state privacy laws define precise location data as data collected from a device that is capable of identifying a consumer's location within a radius of 1,850 feet (or less in some states). This data is considered sensitive personal information and requires companies to obtain opt-in consent, provide notice at collection, adhere to stringent data minimization requirements, and comply with additional obligations. In contrast, non-precise location data, such as city or ZIP code-level, is generally not treated as sensitive and may be used under more typical notice and opt-out frameworks.

Regulators and litigators are increasingly focused on improper or undisclosed use of precise location data, particularly in contexts where users would not expect tracking (eg, apps with no clear need for location access), where the data reveals sensitive inferences (eg, visits to clinics, religious institutions, or political events), or where the data is used in ways that violate the original purpose of collection (eg, using an opt-in for weather updates to deliver personalized ads). Enforcement has also targeted the collection and use of precise location data shared through real-time bidding ('RTB') exchanges and data broker ecosystems, underscoring the importance of evaluating both data source and use.

7.8 How are data brokers defined and regulated under privacy law?

While definitions vary by law, data brokers are generally defined as companies that collect and sell or license personal data to third parties about consumers with whom they do not have a direct relationship. For a summary of applicable laws, see question 1.2.

Data brokers must register annually in public data broker registries maintained by California, Vermont, Texas, and Oregon, pay a fee, and provide transparency about their data practices. Beginning in 2026, California's Delete Act will require data brokers to check the state's Delete Requests and Opt-Out Platform every 45 days and delete the personal data of consumers who have submitted valid opt-out requests. This requirement may cause operational difficulties, as many data brokers rely on pseudonymous identifiers and may not be able to easily match records to opt-out requests.

Companies that engage with data brokers also have obligations, including conducting due diligence to ensure data was collected lawfully, honoring consumer rights, and executing contracts with appropriate data provisions. To the extent data brokers export consumer data outside the US, they may be subject to additional obligations under federal data transfer laws.

Enforcement efforts increasingly target data brokers, especially those involved in the sale or repurposing of sensitive personal data such as precise location or health data.

7.9 How is advertising to children and minors regulated under privacy law?

While definitions vary by law, data brokers are generally defined as companies that collect and sell or license personal data to third parties about consumers with whom they do not have a direct relationship. For a summary of applicable laws, see question 1.2.

Data brokers must register annually in public data broker registries maintained by California, Vermont, Texas, and Oregon, pay a fee, and provide transparency about their data practices. Beginning in 2026, California's Delete Act will require data brokers to check the state's Delete Requests and Opt-Out Platform every 45 days and delete the personal data of consumers who have submitted valid opt-out requests. This requirement may cause operational difficulties, as many data brokers rely on pseudonymous identifiers and may not be able to easily match records to opt-out requests.

Companies that engage with data brokers also have obligations, including conducting due diligence to ensure data was collected lawfully, honoring consumer rights, and executing contracts with appropriate data provisions. To the extent data brokers export consumer data outside the US, they may be subject to additional obligations under federal data transfer laws.

Enforcement efforts increasingly target data brokers, especially those involved in the sale or repurposing of sensitive personal data such as precise location or health data.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

US privacy law does not currently provide a unified framework for regulating profiling, AI, or ADMT in advertising. Most existing and proposed legal frameworks focus on automated decisions that produce legal or similarly significant effects, such as those involving access to housing, employment, credit, insurance, education, healthcare, or other essential services. In those contexts, companies may be required to provide opt-outs, disclose their use of ADMT, and conduct risk assessments.

Although most advertising use cases do not fall within that high-impact category, companies using AI or profiling for advertising must still comply with applicable privacy laws. As referenced above, US privacy laws are technology agnostic, meaning companies are expected to meet legal obligations, such as notice, consent, and consumer rights, regardless of whether the processing is carried out by humans, rules-based systems, or machine learning models.

A growing number of states are introducing or passing laws to regulate AI and ADMT. For example, California has proposed draft regulations that would apply to ADMT used for advertising, including consumer notice and opt-out requirements. Colorado's AI Act, enacted in 2024, imposes a duty of care on developers and deployers of high-risk AI systems to prevent algorithmic discrimination and ensure transparency. These laws may not apply broadly to advertising, but could affect use of ADMT in regulated or high-risk sectors.

In parallel, the FTC has emphasized through guidance and enforcement that overstating the functionality, accuracy, or privacy protections of AI tools can constitute a deceptive trade practice. Businesses must ensure that AI-driven outputs are not misleading and that decisions made by automated systems are fair and transparent.

7.11 Are there other specific advertising practices that you wish to discuss?

Our thought on specific advertising practices are sufficiently covered throughout this chapter.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes. The United States restricts or prohibits transfers of bulk sensitive US data (eg, device identifiers, precise geolocation) to countries of concern (China, Russia, Iran, North Korea, Cuba, Venezuela) or to covered person (entities in or controlled by those countries), even if the data is anonymized or de-identified. Companies in the advertising ecosystem that share data with vendors, such as through SDKs

that collect ad IDs or precise location data, should conduct due diligence, apply appropriate technical restrictions, and updating agreements as necessary to comply with the law. For a summary of applicable laws, see question 1.2.

In addition, many comprehensive state privacy laws require contractual limitations on data use. While there is no direct US equivalent to the European Union's standard contractual clauses, these laws often mandate data processing addendums or specific contractual provisions, and data transfers may also be limited by what is disclosed in a company's privacy policy.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Privilege concerns can complicate the sharing of attorney-client communications or other sensitive information with entities in jurisdictions that do not recognize US legal privilege protections. Further, data localization laws in certain countries may also conflict with US transfer rules, requiring businesses to carefully assess where data is stored and processed.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in the United States? Are there minimum standards? Does this differ by sector or size of the entity?

Data security is regulated through a patchwork of federal and state laws, with no single, comprehensive national standard. The FTC enforces general requirements for most commercial entities, requiring them to implement reasonable technical, administrative, and physical safeguards to protect sensitive personal data, such as health, financial, biometric, and geolocation data, from unauthorized access, use, or disclosure.

At the state level, several jurisdictions have enacted more specific security requirements. For example, Massachusetts requires regulated entities to maintain a comprehensive written information security program, including encryption requirements for data in transit and on portable devices. New York's SHIELD Act sets minimum security obligations for safeguarding private information, though it does not mandate specific technical controls—instead, it provides a safe harbor for businesses that implement certain security practices.

Sector-specific regulations often impose their own detailed security standards, including mandatory risk assessments, encryption, and periodic audits. Taken altogether, the data security regulatory landscape emphasizes the adoption of reasonable, risk-based measures tailored to the sensitivity of the information and the context of its use.

9.2 How are personal data breaches regulated in the United States? What are the requirements for notification and response?

The US does not have a federal comprehensive data breach law. Certain sectors have their own data breach requirements. Under the Health Information Technology for Economic and Clinical Health Act, which is part of HIPAA, covered entities must notify affected individuals, the HHS, and potentially media outlets of a breach. Under GLBA, a financial institution must notify affected customers promptly after determining nonpublic personal information has been, or will be, misused.

Each of the 50 states, the District of Columbia, Puerto Rico, US Virgin Islands, and Guam have adopted data breach notification laws. The unauthorized access and/or acquisition of statutorily defined

personal information will trigger state data breach notification requirements. The specific definitions and reporting requirements vary by state. Personal information protected by such laws generally includes, at a minimum, an individual's name combined with a social security number, driver's license number, or financial account number in combination with a password to access the account. Many states have expanded the definition to include elements such as username and password for an online account, medical information, biometric information, mother's maiden name, and passport. States typically require written notice to be provided without delay and within 30, 45, or 60 days to all affected individuals, and in some cases to government entities and consumer reporting agencies. Some states require companies to provide credit or identity reporting services to affected individuals.

As requirements for data breach notification vary and misrepresentations in notices may lead to further liability, companies experiencing a data breach should seek legal advice as soon as possible.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties for non-compliance vary significantly depending on the law and the type of violation. The FTC may seek remedies such as cease-and-desist orders, disgorgement, restitution, and civil penalties for repeat violations or under specific statutes like COPPA or FCRA. In contrast, many sectoral laws permit penalties for first-time offenses. Agencies like the CFPB, HHS, and FCC have all imposed monetary penalties for privacy and data security violations within their jurisdictions.

State privacy laws often authorize civil penalties, injunctive relief, or corrective actions. For example, the CCPA authorizes penalties of up to USD 2,500 per violation or USD 7,500 per intentional violation, enforceable by the California AG and the CPPA.

10.2 Do consumers have a private right of action? What remedies are available to them?

In the US, consumers have limited private rights of action under privacy laws, and the remedies available vary significantly depending on the statute.

Most federal privacy laws do not provide a private right of action, with notable exceptions including TCPA (texts) and VPPA (video viewership data), which allow for statutory damages.

Similarly, most comprehensive state privacy laws do not include a private right of action. The only exception is CCPA, which provides a limited private right of action for certain data breaches involving non-encrypted, non-redacted personal data. Statutory damages can reach up to USD 750 per consumer per incident or actual damages, whichever is greater.

Some sector-specific state laws allow for private suits. For example, BIPA (biometrics) provides a strong private right of action with statutory damages of USD 1,000 per negligent violation and USD 5,000 per intentional or reckless violation. The CIPA, California's wiretapping statute, provides a private right of action with statutory damages of USD 5,000 per violation.

Even where no statutory privacy right exists, consumers may still bring claims under common law theories such as breach of contract, negligence, or invasion of privacy. Some litigators have also pursued unfair or deceptive acts or practices claims under state consumer protection laws, including those predicated on alleged COPPA violations, though these typically require showing actual damages.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

US privacy regulators at both federal and state levels have become increasingly active in enforcing privacy-related practices, particularly in the advertising ecosystem. Regulatory focus has intensified around data sharing, tracking technologies, use of sensitive personal data, and disclosures in ad tech.

At the federal level, the FTC has brought numerous high-profile enforcement actions against data brokers, app developers, and advertising platforms. In 2022, the FTC filed suit against Kochava, a data broker accused of selling precise location data without consumer consent, potentially exposing visits to sensitive locations such as reproductive health clinics or places of worship. In 2024, the FTC reached settlements with X-Mode Social and Mobilewalla, both of which allegedly collected and sold location data through SDKs embedded in mobile apps, often without adequate notice or user control.

The FTC has also prioritized enforcement related to the use of health data in advertising. In 2023, the agency settled with GoodRx, after alleging that the company shared consumers' health data, including prescription data, with advertising platforms (eg, Facebook, Google) via tracking pixels, without consent. That same year, the FTC brought an action against BetterHelp, alleging the online therapy provider shared sensitive mental health intake data with platforms such as Meta and Snapchat to fuel targeted advertising campaigns. GoodRx paid a USD 1.5 million penalty, while BetterHelp paid USD 7.8 million in consumer redress and was prohibited from using health data for advertising purposes.

At state level, California has led the way: its AG has brought multiple enforcement actions under the CCPA. In Sephora (2022), the AG secured a USD 1.2 million settlement for alleged failure to disclose data sharing with ad tech partners and to honor GPC signals. In DoorDash (2024), the AG alleged the company shared personal data with marketing cooperatives without adequate notice or opt-out, resulting in a USD 375,000 settlement. In Tilting Point (2024), a USD 500,000 settlement resolved claims that the company collected and sold children's and teens' personal data for advertising purposes without consent.

The CPPA has also initiated its own investigations and enforcement. It has brought actions against data brokers for failing to register, and actions against other companies for using dark patterns, operating malfunctioning consent managers, maintaining inadequate contracts, and failing to offer compliant opt-out mechanisms.

Other states are increasingly asserting enforcement authority. Texas, for example, has brought actions under its comprehensive state privacy law. In one case, the state sued a company for collecting and selling vehicle telematics and driving behavior data without proper consumer notice or transparency.

Even states without comprehensive privacy statutes are enforcing more actively. In 2025, Michigan's AG sued for alleged COPPA violations, citing deceptive advertising practices involving children's data.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in the United States?

- (a) **Freedom of speech:** US privacy regulation is often balanced against First Amendment rights, particularly where laws may restrict how companies use data in marketing, publishing, or political contexts. Courts have struck down or limited privacy rules that interfere with commercial speech, shaping how regulators draft and enforce laws.

- (b) **Free market values:** There is a longstanding US preference for market innovation over regulatory intervention, which has influenced a light-touch approach to privacy enforcement in commercial contexts, especially in advertising. Industry self-regulation (eg, NAI, DAA) has historically played a larger role than in many other countries.
- (c) **Individual responsibility:** US privacy law tends to emphasize individual choice over collective protections, favoring notice-and-consent models, opt-outs, and transparency requirements rather than broad default restrictions.
- (d) **Litigation culture:** The US has a robust litigation environment, which shapes corporate privacy strategies. Companies tend to prioritize compliance with laws that carry a private right of action due to the risk of class action lawsuits and statutory damages.
- (e) **National security concerns:** Rising tensions with countries like China, along with a broader retreat from globalization, have led to increased scrutiny of cross-border data flows and foreign access to sensitive data. Recent regulations treat data privacy as a national security issue, not just a consumer protection matter.
- (f) **Political tension:** Privacy debates are increasingly influenced by concerns about how data collection and surveillance disproportionately impact marginalized groups, including women, LGBTQ+ individuals, and communities of color. Following the reversal of *Roe v Wade*, fears have grown over the use of location, health, and online activity data to monitor or penalize those seeking reproductive or gender-affirming care—prompting greater regulatory scrutiny of commercial data practices that may enable discrimination or state overreach.

11.2 What are the ‘hot topics’ or anticipated legal challenges that companies should monitor?

AI and profiling technologies are now central targets of privacy regulation and enforcement. States are advancing laws that impose transparency, risk assessments, anti-discrimination safeguards, and consumer opt-outs for AI systems used in advertising and other business practices. Businesses using AI-driven marketing tools must navigate a growing patchwork of state-level requirements, including annual impact assessments and disclosures for high-risk uses.

Additionally, while Congress fails to act on privacy or AI, numerous states are rolling out or enforcing new privacy laws, and AGs are pursuing aggressive actions involving children’s data, health and location tracking, and AI-driven advertising. The result is a fragmented, fast-moving regulatory environment that requires continuous monitoring and state-by-state compliance strategies.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

Privacy compliance is no longer just a legal issue. It requires collaboration across legal, marketing, product, security, and data teams. Clear internal processes, education, and governance structures are essential to ensure compliance is reflected in real-world product behavior.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The number of US states with comprehensive privacy laws has expanded rapidly, largely triggered by Congress’s continued failure to pass a federal privacy law. As privacy law has matured, consumer awareness has grown, and state regulators have significantly increased enforcement activity.

Federally, new laws and regulations now restrict cross-border data flows, driven by geopolitical concerns, a retreat from globalization, and data increasingly being viewed as a national security asset.

Additionally, there has been heightened regulatory attention on sensitive data largely due to their potential for significant harm if misused. The FTC and state regulators have highlighted this area through enforcement efforts, leading to stricter consent requirements, enhanced transparency obligations, and tighter controls on sensitive data.

The widespread deployment of AI has prompted states to introduce new rules requiring transparency, risk assessments, opt-outs, and anti-discrimination protections. These shifts were triggered by growing concerns over algorithmic bias, surveillance, and opaque data use across many industries.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The rapidly evolving privacy landscape presents significant challenges for businesses, driven by new state, federal, and international laws. Without a federal standard, businesses must navigate differing requirements for consent, consumer rights, data minimization, and security, raising compliance complexity and cost. Cross-border data transfers have become more regulated, requiring robust safeguards and transparency for international data flows or face penalties. AI and ADMT add another dimension, as companies must address new transparency and fairness obligations.

12.3 What do you envision the privacy landscape will look like in five years?

The privacy landscape will become more complex, but also more established and predictable. The absence of a US federal privacy law will lead to further state-level legislation, adding to the patchwork of rules businesses must navigate. Globally, governments will expand privacy and AI governance rules in response to new technologies and business models. Meanwhile, privacy compliance will become more standardized in business operations, like established norms in data security, healthcare, and financial services. As regulators gain experience and expectations solidify, penalties for noncompliance will increase, with less leniency for companies that fail to implement basic privacy practices.

 URUGUAY

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Uruguay.

Data protection in Uruguay is regulated through different instruments:

- (a) Firstly, the following articles of the Constitution have been interpreted as granting a constitutional standing to the right to privacy, as a right that is inherent to the human person:
 - (i) Article 72, which provides that ‘the enumeration of rights, duties and protections established in the Constitution, does not exclude other rights that are inherent to the human personality or are derived from the republican form of government’; and
 - (ii) Article 332, which states that ‘the application of the precepts of this Constitution that acknowledge individuals’ rights, as well as those awarding rights and imposing obligations on public authorities, shall not be impeded by the lack of pertinent regulations, but rather this will be substituted through recourse to the underlying bases of similar laws, to the general principles of law and generally accepted doctrines’.
- (b) Secondly, there are also some particular laws and decrees that regulate privacy (see question 1.2).
- (c) Finally, some of the opinions issued by the Uruguayan data protection regulator, URCDP, are also applicable, such as the guidelines for the use of video surveillance, drones or cookies, bring your own device, the guidelines for data dissociation, and recommendations for using messaging applications, among others.

1.2 What are the primary laws regulating privacy in Uruguay? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The key regulation on personal data protection in Uruguay is Law No 18,331 on the Protection of Personal Data and Habeas Data Action (the ‘DPL’) and its Regulatory Decree.

There are no special regulations on data protection aspects for advertising activities.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

There are currently no relevant self-regulatory bodies.

1.4 How is privacy law enforced in Uruguay? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Uruguay’s data protection regulator, URCDP, is an autonomous entity of the Agency for the Development of Electronic Government Management and the Information and Knowledge Society (‘AGESIC’).

However, as mentioned above, Uruguay has no relevant self-regulatory bodies.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Uruguay?

In Uruguay, a company is subject to the DPL when it processes personal data recorded in any format that renders them subject to processing, as well as to any subsequent use of such data.

The following are not subject to the provisions of this law:

- (a) those maintained by natural persons in the exercise of activities that are exclusively personal or domestic;
- (b) databases whose purpose is public security, defense, state security, or activities related to criminal investigation and prosecution; and
- (c) databases created and governed by special laws.

All companies that meet the requirements for the application of the DPL may be subject to it, both regarding the obligations it imposes and rights it grants. Please note that legal entities may be considered 'data subjects', and thus their personal data is also protected under the DPL, where appropriate.

2.2 Does privacy law in Uruguay apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

The DPL applies to companies not established in Uruguay in the following cases:

- (a) the data processing activities are targeted at offering goods or services to Uruguayan inhabitants, or are intended to analyze their behavior;
- (b) the DPL is the applicable law under an agreement or under international public rules; or
- (c) the processing activities are carried out by means located in Uruguay, unless these means are only used for transit and the data controller appoints a local responsible person.

There are no obligations stated in the DPL particular to companies outside Uruguay.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Uruguay?

'Personal data' is defined as information of any kind relating to natural persons or legal entities, determined or determinable.

Please note that, in order for such a piece of information not to be considered personal data, URCDP considers that it must be irreversibly dissociated.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

'Sensitive data' includes personal data revealing racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership, and information relating to health or sex life.

The DPL provides a more restrictive regime for the treatment of this kind of data, establishing an obligation to obtain the data subject's express written consent.

In addition, a company processing sensitive data as its main business is one of the circumstances under which a company must appoint a data protection officer before URCDP. Also, processing sensitive data

as its main business, or the permanent or regular processing of specially protected data (which includes sensitive data), may also imply the necessity for a company to carry out a data protection impact assessment ('DPIA').

'Biometric data' is personal data obtained from a specific technical treatment, related to the physical, physiological or behavioral aspects of a natural person which allow or confirm the unique identification of that person; examples include fingerprint data, image or voice recognition. A privacy impact assessment must also be carried out when processing this kind of personal data.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

In this regard, URCDP has issued Guidelines on Data Anonymization. The DPL does not establish detailed legal requirements for the technical implementation of anonymization. However, the underlying legal standard is clear: for data to be considered anonymized and fall outside the scope of personal data protection regulations, the anonymization process must make re-identification impossible by any reasonable means. According to URCDP's guidelines, achieving this level of anonymization requires a combination of appropriate technical methods and privacy models that are selected based on the nature of the dataset and the intended use of the anonymized data.

Moreover, organizations are expected to evaluate the residual risk of re-identification on an ongoing basis and apply additional safeguards when necessary. This includes limiting access to anonymized datasets, defining clear usage purposes, and updating anonymization strategies in response to new threats or technologies.

In short, the legal requirement is not tied to a specific technique but rather to the outcome: anonymized data must be demonstrably and sustainably untraceable to any identifiable individual.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The key principles set out in the DPL with which companies must comply are:

- (a) **Legality:** Data controllers have the obligation to register a database before URCDP in order for it to be lawful. In addition, a database cannot have purposes that infringe human rights or are contrary to law or public morals;
- (b) **Veracity:** Personal data that is collected has to be truthful, adequate, fair, and not excessive in relation to the purpose for which it was obtained. The collection of personal data may not be done by unfair, fraudulent, or abusive means, extortion nor in a manner contrary to the provisions of URCDP;
- (c) **Purpose limitation:** Personal data must not be used for purposes that are different from or inconsistent with those that led to their collection. When the data is no longer necessary or relevant for the purpose for which it was collected, it must be removed;
URCDP allows certain exceptions to the limitation on retention, such as when the data has value for historical, statistical, or scientific reasons;
- (d) **Prior consent:** See question 4.3;
- (e) **Data security:** The data controller or user of the database must take the necessary steps to ensure the security and confidentiality of the personal data, and prevent alteration, loss, consultation or unauthorized processing;

- (f) **Non-disclosure:** Persons and organizations that hold personal data must keep it confidential, and use it exclusively for the operations of their normal activity. All other dissemination of the data to third parties is prohibited; and
- (g) **Responsibility:** The data controller and the data processor are responsible for the violation of any provision of the DPL. Thus, interested parties who have suffered damage as a consequence of the processing of their personal data may request the relevant redress. In addition, in compliance with a proactive responsibility, the DPL also states that both data controllers and data processors must take all the appropriate technical and organizational measures (eg, privacy by design and by default, privacy impact assessment, among others) in order to guarantee an adequate processing of the personal data, as well as to demonstrate its effective implementation.

Further, although there are no specific provisions to that effect in the DPL, when carrying out data processing activities, transparency and data minimization are also recommended. The adopted measures must be documented and periodically reviewed, and their effectiveness needs to be assessed. Some requisites on the documentation of these measures must also be met.

The key obligations under the DPL are the following:

- (i) registering the databases before URCDP;
- (ii) complying with the principles stated in the DPL (see above);
- (iii) responding as required to data subjects when they exercise any of their rights under the DPL (see question 5.2);
- (iv) when processing personal information for marketing or advertising communications, only using personal data that is available in public sources, or has been provided by the data subject or obtained with their consent;
- (v) informing data subjects about their right to request a block on, or removal of, their personal information from marketing and advertising listings;
- (vi) (when the entity processes sensitive data as its main business, or processes large volumes of data (meaning personal data of more than 35,000 data subjects)) appointing a data protection officer before URCDP. The main functions of a data protection officer are:
 - to advise on the design and appliance of privacy policies,
 - to oversee the fulfilment of the data protection framework,
 - to recommend any measurements to comply with the international framework and standards regarding privacy, and
 - to act as a point of contact between its entity and URCDP;
- (vii) carrying out privacy impact assessments in those cases required by the DPL (among which processing personal data for marketing purposes is specifically mentioned) or when URCDP deems it convenient;
- (viii) implementing privacy by design and by default measures;
- (ix) when processing personal data through a website, making the privacy policy about the data processing available;
- (x) when a data breach occurs, initiating the necessary procedures to minimize the impact of said incident within the first 24 hours of verification;
- (xi) notifying data securities breaches to URCDP within 72 hours and also to the data subjects;
- (xii) not contacting by telecommunication services, for advertising, offer, sale, gift of goods or services, people who have not requested it and who have registered in the Do Not Call Registry before the Communications Services Regulatory Unit ('URSEC') (see question 7.1).

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The DPL distinguishes between data controllers and data processors:

- (a) **Data controllers** are defined as the natural person or legal entity, public or private, who owns the database or who decides on the purpose, content, and use of the data treatment;
- (b) **Data processors** are defined as the natural person or legal entity, public or private, who alone or together with others, processes personal data on behalf of a data controller.

There are some differences between the obligations of a controller and processor. For instance, it is the controller who has the obligation to register databases before URCDP in compliance with the principle of legality, not the processor. However, in general terms, the obligations provided in the DPL extend to both data controllers and processors.

Regarding contractual requirements, note that, although in the DPL there is no specific obligation to do so, it is understood that data processing agreements must be signed to formalize the obligations and responsibilities of each party. International data transfers agreements to countries that are not considered to provide adequate levels of protection must include certain requirements recommended by URCDP (see question 8.1).

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

As a general rule, the processing of personal data is permitted only if the data subject has given their free, prior, explicit and informed consent, which must be documented. There are certain exceptions to the principle, in which consent is not required, such as:

- (a) when the data comes from public sources of information specifically mentioned in the DPL, such as registries or publications in mass media;
- (b) when the data is collected for the performance of functions of the government or under a legal obligation;
- (c) (for listings of natural persons) those that are limited to name, identity document, nationality, address, and date of birth, or (for listings of legal entities) those limited to corporate name, brand name, tax identification number, address, phone number, and identity of the people in charge;
- (d) when the data derives from a contractual, scientific or professional relationship of the data subject, and is necessary for its development or execution; or
- (e) when the treatment is carried out by a natural person for their own personal and domestic use.

Note that, when referring to consent for data processing, the data subject must be provided with a way to give or refuse their consent which is simple, clear and free of charge. In that regard, it is understood that the obligation to obtain consent is fulfilled when the data subject is given the opportunity to choose between two clearly identified options, which cannot be pre-marked, whether in favor or against. Furthermore, in Uruguay, legitimate interest does not constitute a valid legal basis for data processing; instead, processing must be grounded in the explicit consent of the data subject.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Companies processing personal data for advertising purposes must include specific information in their privacy notices to comply with the DPL and related regulations, this mainly includes the following information:

- (a) **Data controller:** the entity responsible for processing personal data must be clearly identified;
- (b) **Purpose:** the specific reason for collecting data and the aim of processing it;
- (c) **Retention period:** the duration for which personal data will be stored;
- (d) **Data collection:** details on the types of personal data being gathered (eg, name, age, address, gender, etc). If personal data from minors is collected, prior authorization and consent from their legal guardians is required;
- (e) **International data transfers:** whether personal data will be transferred to other entities or jurisdictions;
- (f) **Rights of data subjects (ARCO rights):** consumers have:
 - (i) the right to access,
 - (ii) the right to erasure,
 - (iii) the right to update,
 - (iv) the right to rectify,
 - (v) the right to include, and
 - (vi) the right to information.

The data controller must respond to a request from a data subject within five business days. Otherwise, the data subject has the right to start an action in habeas data; and
- (g) **Security measures:** that the data controller has implemented appropriate mechanisms to protect the collected information.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

In advertising contexts, consumers have the following rights:

- (a) **Prior consent:** Companies must obtain the consumer's consent before collecting and using their personal data for advertising purposes.
- (b) **Purpose:** Companies must inform consumers about how their data will be used, including any international transfers.
- (c) **Security measures:** Data controllers are required to implement measures to protect the collected information.
- (d) **ARCO rights:** See question 5.1(f).

Data subjects also have the right to block/remove personal data from marketing listings. No reason is needed to exercise this right, which is to be implemented immediately.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See question 4.3. Companies must always obtain consent when processing personal data apart from the exceptions described in question 4.3. Hence, the data subject must give their free, prior, explicit and informed consent, which must be documented.

The circumstances and measures required are:

- (a) **Explicit consent for targeted advertising:** If a company wants to use personal data for direct marketing or targeted advertising, it must obtain informed and voluntary consent from the individual.
- (b) **Opt-out mechanisms:** Consumers must be given the option to withdraw their consent at any time and opt out of receiving advertising communications. This implies the right to erasure, which is one of the ARCO rights.
- (c) **Transparency requirements:** Companies are required to provide individuals with transparent information regarding the intended use of their personal data, including any potential sharing with third parties or transfers across international borders.
- (d) **Proactive responsibility and security measures:** Data controllers and processors must implement measures to ensure compliance with regulations, including privacy by design and by default, as well as conducting privacy impact assessments.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Privacy law regulates the use of vendors and third parties in advertising as follows:

- (a) The communication of personal data to a third party can be done only with the prior consent of the data subject (save for the exceptions described in question 4.3).
- (b) Companies should ensure that third-party vendors process personal data on a valid legal basis, such as user consent. The data subject should be informed of the purpose of the communication and the identity of the recipient, or the elements that allow for such identification, as well as of the activities developed by the recipient. Consent is revocable. Prior consent for sharing personal data with a third party is not necessary:
 - (i) when provided by a law of general interest;
 - (ii) when consent is not required for data processing;
 - (iii) (regarding health data) when communication is necessary for health or emergency reasons, or for carrying out epidemiological studies, as long as the data subject's identity is preserved by using adequate dissociation mechanisms when applicable; or
 - (iv) when personal data is dissociated, the data subjects are not identifiable.
- (c) Companies should establish contracts with advertising agencies, DSPs, SSPs, and data providers which ensure compliance with the DPL, and responsibilities and security measures are established. Note that companies remain responsible for ensuring that third parties comply with security and privacy standards.
- (d) Companies must disclose the involvement of third parties in their privacy policies, informing users about data transferring.
- (e) If operating outside Uruguay, companies must verify that the receiving country provides an adequate level of data protection. See question 8.1.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Companies must comply with the following obligations when processing personal data to or from vendors/third parties:

- (a) Confidentiality must be maintained regarding the personal data accessed;
- (b) The data may not be used for a purpose other than that for which it was transferred;
- (c) Necessary technical and organizational measures must be adopted to ensure data security and prevent alteration, loss, theft, processing, or unauthorized access;
- (d) Once the contractual relationship granting access to the data has ended, all related information must be either destroyed or returned, considering various storage formats such as database disks, temporary files, backups, or paper documents;
- (e) In the event of a security breach affecting personal data, the following must be done:
 - (i) necessary technical measures must be taken to minimize the impact of the breach and immediately investigate the situation (see question 9.2), and
 - (ii) the other party must be informed about the incident.
- (f) Personal data must be processed in the territory designated for such processing; and
- (g) Data may not be transferred without prior authorization, considering that personal data must always be processed in countries that URCDP deems to provide sufficient protection levels.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies are expected to implement due diligence measures to ensure compliance with data protection laws when handling personal data. These measures imply:

- (a) evaluating potential privacy risks associated with data processing activities;
- (b) establishing internal policies to govern data collection, storage, and sharing;
- (c) ensuring that third-party vendors comply with the DPL and maintain adequate security measures;
- (d) private training of staff handling personal data in order to prevent breaches and unauthorized access; and
- (e) conducting periodic audits to verify compliance with privacy regulations.

A DPIA is required when advertising activities involve high-risk data processing, such as:

- (i) the use of sensitive personal data as a core business activity;
- (ii) the stable or permanent processing of specially protected data (eg, health data, biometric data, etc);
- (iii) the evaluation of data subjects' personal aspects with the purpose of creating or using personal profiles, particularly through the analysis or prediction of aspects such as job performance, economic situation, health, personal preferences or interests, reliability or behavior, creditworthiness, or location;
- (iv) the processing of data belonging to vulnerable groups, particularly minors or persons with disabilities;
- (v) the processing of large volumes of personal data (ie, personal data of more than 35,000 data subjects); and
- (vi) international data transfers to countries or organizations without an adequate level of protection.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The DPL states that, in the collection of addresses, the distribution of documents, advertising, commercial prospecting, selling or other similar activities, personal data can be used that is suitable to establish specific profiles with promotional, business or advertising purposes or that helps determine consumer habits. This is with the proviso that the personal information concerned is available on publicly accessible documents or is provided by the data subjects themselves or obtained with their consent.

The DPL also states that a data subject may exercise the right of access free of charge and may, at any time, request the removal or blocking of their data from databases.

In addition, Law No 19,996 created the Do Not Call Registry within URSEC, providing a list of the telephone numbers of those who do not wish to be contacted through telecommunications services for the purpose of unsolicited advertising, offers, or gifts of goods or services. A person who does not want to receive such contact must register with their service provider and the service provider must then inform URSEC within 5 days.

Companies must register with URSEC and enable a user to be able to consult the Registry.

Where a person has not registered in the Registry, unsolicited contact must be limited to Monday to Friday 9am–9pm, and Saturdays 9am–7pm, unless otherwise requested by them.

Even where a person is registered in the Registry, contact can continue to be made if:

- (a) expressly permitted by the person,
- (b) free, express and informed consent was obtained, or
- (c) there is a current contractual relationship, and the contact refers to this relationship.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Whilst the DPL does not specifically refer to tracking technologies, as long as the technologies process personal information, the DPL and its provisions will apply.

Moreover, URCDP has issued some guidelines for the use of cookies and drones:

- (a) In general terms, the guidelines on the use of cookies state that the principles recognized under the DPL apply when implementing cookies, as does the data subject's right to information. According to the guidelines, in compliance with the right to information, data subjects must previously authorize the placement of cookies, which must also be limited to the purpose duly informed to the data subject.
- (b) The guidelines on the use of drones state that the entity responsible for the use of the drone must be defined, and that such responsible entity must take the necessary measures in order to comply with data protection regulation and to guarantee the confidentiality and the security of the data. The guidelines also provide that the purpose limitation principle must be considered, under which the personal data cannot be used for purposes other than or incompatible with those for which it was collected.

7.3 How are loyalty programs and promotions regulated under privacy law?

There are no particular data protection provisions regulating loyalty programs and promotions. However, the DPL will apply in cases where personal data is processed in such programs or promotions.

Also note that every website that carries out data processing in Uruguay (such as when the enrolment in a loyalty program or promotion is done through a website) must publish the conditions related to such processing, in accordance with the DPL.

7.4 How is social media and influencer marketing regulated under privacy law?

In Uruguay there are no particular data privacy rules governing social media.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Please see question 7.1.

Also note that it may be necessary to carry out a privacy impact assessment when the data processing implies the evaluation of personal aspects of the data subjects with the purpose of creating or using personal profiles, particularly through the analysis or prediction of aspects related to their preferences or personal interests, inter alia.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

There are no specific regulations governing digital identity resolution or clean room technologies.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising does not have specific regulations but is governed by the general data protection principles established in Law No 18.331. Companies using geolocation data for advertising purposes must obtain the user's prior and explicit consent before collecting and processing their location. It is also mandatory to provide clear and transparent information about how the data will be used, who will have access to it, and how long it will be stored. Additionally, appropriate security measures must be implemented to protect this information from unauthorized access or misuse.

7.8 How are data brokers defined and regulated under privacy law?

In Uruguay there are no particular privacy rules governing data brokers.

7.9 How is advertising to children and minors regulated under privacy law?

In addition to the overall obligations related to data privacy protection for individuals, companies must specially comply with the following:

- (a) A DPIA is necessary when it involves the processing of data belonging to vulnerable groups, particularly minors or people with disabilities;
- (b) Consent and authorization must be obtained from their legal guardians; and
- (c) Minors' data must not be used for advertising or any other purpose linked to alcohol or drugs.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

When processing personal data for advertising purposes, such as profiling, the controller must:

- (a) enable the data subject's right to access their personal data at any time, free of charge;
- (b) permit the data subject to withdraw their consent or request the blocking of their personal data at any time;
- (c) conduct a DPIA;
- (d) if profiling is involved, the controller must inform the data subjects about these purposes of processing. This includes how profiles are created, their purposes, who is responsible for them, and how data subjects can exercise their rights related to personal data protection; and
- (e) if automated data processing is involved, the controller must provide information regarding the assessment criteria, the processes applied, and the technological solution or software used. In addition, the controller must enable data subjects to exercise their right not to be subject to a decision that may have a significant impact on their rights.

There is no specific regulation regarding the use of artificial intelligence. However, it is expected that legislation on the matter will be developed in the near future.

7.11 Are there other specific advertising practices that you wish to discuss?

There are no additional advertising practices that have not been covered

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

The DPL states that cross border personal data transfers to countries that do not provide adequate levels of protection, according to the standards of international or regional law, are prohibited.

There has been an update of the list of adequate countries for international data transfers which established that the countries that provided adequate levels were the United Kingdom, those of the European Union, and those to which the European Commission has granted the 'adequacy note' (namely: Switzerland, private sector of Canada, Guernsey, Isle of Man, Jersey, Faeroe Islands, Argentina, Andorra, Israel, Japan and New Zealand). However, the list of countries considered adequate for international transfers has been expanded to include entities subject to the Personal Information Protection Act of the Republic of Korea and entities included in the Data Privacy Framework. In that sense, the controller must submit to URCDP a declaration from the importing entity confirming that it extends the safeguards of the Data Privacy Framework to the data transferred from Uruguay for the transfer to be considered adequate. Data transfers to companies located in the United States that have adhered to the Privacy Shield Agreement are no longer considered lawful. Thus, some measure has to be taken to legitimize such transfers.

Cross-border data transfers carried out within a multinational company between affiliates, between subsidiaries, and between any of them and their parent company, are considered lawful, as long as a code of conduct of professional practice on the matter has previously been registered before URCDP.

URCDP has provided a series of clauses that international data transfer agreements must include where data is being transferred to countries that are not considered to provide adequate levels of protection.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Some other limitations on the processing of data outside Uruguay may apply, depending on the industry in which the data controller is operating. For instance, institutions regulated by the Uruguayan Central Bank ('UCB') may require the prior authorization of UCB. Among other aspects to be considered in such cases is whether data processing abroad is considered substantial or not.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Uruguay? Are there minimum standards? Does this differ by sector or size of the entity?

Under the principle of data security the data controller or user of the database must take the necessary steps to ensure the security and confidentiality of the personal data. Such measures must prevent the alteration, loss, consultation or unauthorized processing of the data, as well as detect any redirection of information, intentional or not, whether the risks come from human action or from the technical means used.

No particular measures are prescribed. However, AGESIC (of which URCDP is a decentralized body) recommends the implementation of the ISO/IEC standards regarding information security. To that end, a set of guidelines for the enforcement of the DPL according to the ISO/IEC standards has been developed for organizations to use as recommendations to comply with the DPL. In addition, Decree No 64/020 states that the implementation of national and international standards on data security (such as the Framework for Cybersecurity prepared by AGESIC) will be well appreciated.

The adopted measures must be documented and periodically reviewed, and their effectiveness must be analyzed. The documentation must comply with certain requisites; for example, it must include the means and purpose of the data processing, inter alia. The documents should be available on request to URCDP.

9.2 How are personal data breaches regulated in Uruguay? What are the requirements for notification and response?

According to the DPL, a data security breach must be reported immediately, in detail, both by data controllers and by data processors, as soon as they become aware of the breach. Where a data processor becomes aware of a data breach, they must immediately inform the data controller of the situation. The controller will then notify those data subjects whose rights have been significantly affected.

The DPL states that the concept of 'security breach' includes, inter alia, breaches that cause the disclosure, destruction, loss or accidental or unlawful alteration of personal data, or unauthorized communication or access to such data. Where a breach occurs, the necessary procedures in order to minimize the impact must be taken within the first 24 hours after becoming aware of the incident. In addition, a notification must be addressed to URCDP within 72 hours and to all affected data subjects,

and must include details about the breach and the measures taken. The DPL provides that URCDP will coordinate the course of action to be taken with the National Centre for Response to Computer Security Incidents of Uruguay ('CERTUy').

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

URCDP may impose the following punitive measures:

- (a) notice of violation;
- (b) warning (when the infringement is mild and the controller has no previous record of any other infringement);
- (c) fine (when the infringement is mild but there is a record of previous infringements, or where the infringement is severe or very severe);
- (d) suspension of the database concerned (when the infringement is very severe); and
- (e) closure of the database concerned (when the infringement is very severe).

The sanctions of suspension and closure of databases are applied when a fine is not adequate to address very severe violations of the DPL.

However, URCDP does not, in practice, have a policy of active control; it acts upon claims submitted by data subjects.

URSEC may impose other penalties for non-compliance with Do Not Call Registry obligations.

10.2 Do consumers have a private right of action? What remedies are available to them?

The DPL establishes that data subjects may bring an action for the protection of personal data or habeas data against any data controller of a public or private database, in cases when:

- (a) the data subject has requested access to their personal information and such access was denied, or was not provided by the data controller in the timeframe and manner established by the DPL, or
- (b) the request of the data subject to have their information corrected, updated, removed, or deleted was not complied with within the timeframe established by the DPL.

The action of habeas data may be exercised by the data subject concerned or by their representatives (guardians or curators), and, in case of deceased persons, by their heirs. In the case of legal persons, the action is brought by their owners or trustees appointed for this purpose.

Although it is not expressly stated in the DPL, data subjects can also submit civil actions regarding data privacy.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In Uruguay, privacy enforcement is actively monitored by URCDP, which oversees compliance with the DPL. URCDP has issued resolutions and sanctions against companies failing to comply with privacy regulations, particularly in cases involving unauthorized data processing and insufficient security measures.

The authority has also intervened in cases involving advertising practices that fail to respect users' preferences, especially when individuals request to stop receiving promotional communications and their choices are not honored. These enforcement trends reveal common patterns such as:

- (a) continuing to send emails or text messages after a person has clearly opted out of receiving marketing content;
- (b) not offering a clear and accessible opt-out mechanism, such as requiring users to go through multiple steps, log in, or fill out unnecessary forms;
- (c) using personal data for marketing purposes without valid consent; for example, by collecting it from public sources and using it for direct advertising without informing the individual;
- (d) sharing personal data with third parties for advertising without being transparent or giving the individual a chance to object; and
- (e) a lack of coordination between internal systems, where one channel may respect the opt-out (eg, email), but others continue sending messages (eg, SMS or calls).

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Uruguay?

No, we do not visualize particular rules that affect privacy which are particular to local culture.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

There are no current 'hot topics' regarding data privacy in our country. However, artificial intelligence has begun to gain significant importance in the objectives of AGESIC, leading us to anticipate that regulatory measures on this matter may soon be introduced.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The DPL also grants data subjects the right not to be subjected to a decision which will have a meaningful legal effect upon them, if the decision is based on data processing, automated or not, intended to evaluate certain aspects of their personality, their job performance, credibility, reliability, or conduct, among other matters. In other words, an individual has the right to know the reasoning behind a decision that may significantly affect them. A data subject may challenge administrative acts or decisions involving a personal evaluation of their behavior, the sole rationale of which is the processing of personal data that provides a definition of their characteristics or personality.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

There have been no significant changes; therefore, we refer to what has been previously mentioned in which we point out that data protection regulation has become stricter, following, in general terms, the EU model which is usually the compass that guides Uruguay on privacy matters. This has prompted Uruguay to introduce certain requisites for data processing even before they have been introduced in Europe (such as the obligation for consent to be unequivocal). Additionally, in comparison with 2022,

data subjects are becoming more aware of their rights under the DPL, as well as the obligations of data controllers/processors. Finally, data subjects continue using the DPL for purposes other than those for which the DPL was conceived (for instance, data subjects sometimes submit a claim requesting the deletion of their personal data from a database in order to accomplish the termination of a contract).

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

The major challenge for companies is to align their commercial processes, related to the value of information, with the provisions and guarantees of data protection regulation. One of the main tasks to be done will be to carry out privacy impact assessments, anticipating the risks of the data processing, and implementing security measures and mechanisms to show compliance to URCDP.

12.3 What do you envision the privacy landscape will look like in five years?

We foresee that, in the next 5 years, compliance with local regulation will continue to increase, as will the number of data subjects' claims before URCDP. We also expect that URCDP will initiate more ex officio investigations.

 VENEZUELA 

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Venezuela.

Regulations are dispersed, and there is no specific law dealing with this subject; however, the right of privacy and personal data protection has constitutional range. The Venezuelan Constitution, drawn up in 1999, was among the first in the region to adopt the habeas data mechanism.

1.2 What are the primary laws regulating privacy in Venezuela? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The following are relevant:

- (a) Constitution of the Bolivarian Republic of Venezuela;
- (b) Criminal Code;
- (c) Civil Code;
- (d) Law of the Supreme Court of Justice;
- (e) Special Law of Cybercrimes; and
- (f) Organic Law for Fair Price.

The Venezuelan Constitution contains several provisions aimed at guaranteeing the protection of, and respect for, the right to privacy. Additionally, under Venezuela's Constitution, ratified international treaties have constitutional rank.

Article 48 of Venezuela's Constitution provides: 'The secrecy and inviolability of private communications in all forms are guaranteed. The same may not be interfered with except by order of a competent court, with observance of applicable provisions of law and preserving the secrecy of the private issues unrelated to the pertinent proceedings.'

Article 60 states: 'Every person is entitled to protection of his or her honor, private life, intimacy, self-image, confidentiality and reputation. The use of electronic information shall be restricted by law in order to guarantee the personal and family privacy and honor of citizens and the full exercise of their rights.'

However, the solid principles established in the Constitution have not been developed in subsequent and specific laws.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Self-regulation is paramount since there is no specific administrative entity responsible for privacy matters, and regulators have a wide range of action on matters directly or indirectly connected with privacy, especially when connected to advertising topics.

1.4 How is privacy law enforced in Venezuela? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Most privacy cases are decided in civil or criminal jurisdiction, and the courts will determine any applicable precautionary measures, depending on the specific case.

However, on ex-officio procedures, agencies with possible jurisdiction in the administrative field are:

- (a) SUNDDE (this agency mostly deals with fair price issues, but also with a few consumer protection matters);
- (b) CONATEL (telecommunications body, with jurisdiction over a range of matter related with adverting); and
- (c) the Anti-Monopoly agency, with jurisdiction on claims related with deceptive advertising.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Venezuela?

All entities conducting activities in Venezuela are subject to the constitutional principles ruling on privacy law matters, even if those activities are executed through a representative (ie, a distributor or franchisee).

2.2 Does privacy law in Venezuela apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Wherever an initiative, whether commercial or not, is addressed at Venezuelan residents, the local courts/agencies can claim jurisdiction, provided that Venezuelan persons or entities domiciled in the country are affected.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Venezuela?

Personal information/data is all information/data about any individual and/or that individual's assets.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

There is no further development of the rights set out in the Constitution, which is the reason why all cases must be reviewed on their own available facts. The authorities will have a wide level of interpretative discretion when determining whether certain information/data about any individual is sensitive, and thus subject to special protection.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Since there is no specific law for privacy matters, each matter is subject of specific review, based on the nature of the case.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

Key obligations are:

- (a) gaining prior consent;

- (b) availability of applicable documents in Spanish; and
- (c) clear disclosure of the purpose and extent of the use of the data.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

No.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

No.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

When processing personal data for advertising purposes, companies must obtain express consent from the individuals who will be part of the activity. The privacy notice must give details of the purpose of use of the data.

The privacy policy must be available and signed in Spanish.

When it comes to dealing with underage persons, special and mandatory processes must be followed.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Use of data must be limited to specific and detailed circumstances. The rule for interpretation comes from Article 60 of the Constitution (see question 1.2).

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Written consent is always mandatory. See question 1.2.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Depending on the circumstances, third parties are to be considered responsible for any infringement on privacy rights.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

Despite the lack of specific regulation, given that data protection can be interpreted as a fundamental personal right, we advise entities to obtain express consent from individuals regarding these transactions.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

While legislation does not cover the majority of topics of interest related to data privacy, the fact that it is recognized as a constitutional right can never be ignored, and a conservative approach is advised.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Venezuelan law on consumer protection was revoked in 2015, and current legislation does not cover cybersecurity from a consumer rights perspective. However, see question 1.2.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

Tracking technologies are not regulated. However, official agencies are constantly monitoring social and mass media in general.

7.3 How are loyalty programs and promotions regulated under privacy law?

Promotions must offer adequate, truthful, clear, timely, and complete information about goods and services. False, misleading, or abusive advertising is prohibited.

Companies wishing to carry out promotions (offers, discounts, liquidations, etc) need to request authorization from SUNDDE and submit a series of requirements, which may include:

- (a) sworn statement;
- (b) inventory of the merchandise on promotion;
- (c) purchase invoice for gifts or prizes (if applicable), and for the products subject to the promotion;
- (d) cost structure;
- (e) indication of the offer's duration; and
- (f) notarized power of attorney or letter of attorney if the request is on behalf of third parties.

Again, express consent for the use of personal data must be obtained, including approval for sharing such data with third parties.

7.4 How is social media and influencer marketing regulated under privacy law?

Advertising of specific goods (ie, tobacco) and services (gambling) is limited. Content posted on social media is permanently under scrutiny at the sole discretion of regulator(s).

There are no formal rules on influencer marketing.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Targeted advertising is not regulated in Venezuela.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are not regulated in Venezuela.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is not regulated in Venezuela.

7.8 How are data brokers defined and regulated under privacy law?

Data brokers are not regulated in Venezuela.

7.9 How is advertising to children and minors regulated under privacy law?

Any act addressed to, or involving minors, must be subject to express consent from parents/guardians.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

Profiling or the use of AI or automated decision-making technology for advertising purposes are not regulated in Venezuela.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

In spite of a lack of specific regulation, given that data protection could be interpreted as a fundamental personal right, we would advise entities to obtain express consent from individuals regarding these kinds of transactions.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

No.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Venezuela? Are there minimum standards? Does this differ by sector or size of the entity?

No.

9.2 How are personal data breaches regulated in Venezuela? What are the requirements for notification and response?

The Special Law Against Cybercrimes in Venezuela defines general concepts such as data breaches, but there are no specific procedures to handle these matters.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Prison sentences generally range between 1 and 10 years, and fines between 10 and 1,000 Tax Units.

10.2 Do consumers have a private right of action? What remedies are available to them?

Yes, the Habeas Data action, a specific constitutional action derived from Article 28 of the National Constitution. It allows individuals to request a court order to:

- (a) Access their personal data stored in public or private records;
- (b) Know the purpose for which the data was collected and how it's being used;
- (c) Rectify (correct) inaccurate, incomplete, or outdated data;
- (d) Update data; and/or
- (e) Destroy (delete) data that is incorrect or unlawfully affects their rights (this is akin to the 'right to be forgotten' in other jurisdictions, though its scope in Venezuela is more limited and context-dependent).

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

Enforcement of privacy-related matters in Venezuela is significantly less active and less developed compared to other areas. This is primarily due to the absence of a comprehensive, dedicated data protection law and a specialized data protection authority.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Venezuela?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

There is extreme sensitivity from government officers for any matter that could be interpreted as a violation of national sovereignty; and humor, when linked to local events, may be interpreted by them as criticism.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

The level of intervention from public entities has increased.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Understanding the interaction with all governmental agencies with possible jurisdiction on privacy/data matters.

12.3 What do you envision the privacy landscape will look like in five years?

Impossible to predict.

ZIMBABWE

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Zimbabwe.

- (a) The Constitution makes provision for the protection of privacy in sections on right to privacy and access to information.
- (b) The Access to Information and Protection of Privacy Act was enacted by Parliament to deal with the protection of individuals through the prevention of unauthorized collection, use, or disclosure of information by government public bodies and agencies, and gives rights to individuals to access information collected, held and/or maintained by the government. Private entities are not regulated by this Act.
- (c) The long-awaited Cyber and Data Protection Act was enacted and came into operation on December 3, 2021, and is intended to provide for the protection of privacy, and to prevent the unauthorized and arbitrary use, collection, processing, transmission, and storage of data by public and private entities. The intended purposes of the Act are, inter alia, 'to provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest; to establish a Cyber Security Centre; a Data Protection Authority and to provide for their functions; to create a technology-driven business environment and encourage technological development and the lawful use of technology...'.

1.2 What are the primary laws regulating privacy in Zimbabwe? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

The key law for regulation of private entities with respect to privacy is the Cyber and Data Protection Act (see question 1.1).

The Constitution provides that every person has the right to privacy, which includes the right, inter alia, not to have the privacy of their communications infringed. Other laws refer to the protection of privacy and information as a function of other activities or the protection of specific types of rights. These include:

- (a) the Courts and Adjudicating Authorities (Publicity Restrictions) Act;
- (b) the Census and Statistics Act;
- (c) the Banking Act;
- (d) the National Registration Act; and
- (e) the Consumer Protection Act.

There is no self-regulatory framework.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

As there is no self-regulatory framework, self-regulation does not play a significant role in privacy regulation in Zimbabwe. However, advertising practices in Zimbabwe separately are independently self regulated.

1.4 How is privacy law enforced in Zimbabwe? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

Privacy law enforcement in Zimbabwe primarily revolves around the Cyber and Data Protection Act, which establishes a legal framework for data privacy and protection. The Postal and Telecommunications Regulatory Authority of Zimbabwe ('POTRAZ') serves as the primary enforcement body for data protection and privacy. Under the Cyber and Data Protection Act, POTRAZ functions as Zimbabwe's data protection authority, responsible for overseeing compliance, investigating violations, and imposing penalties for breaches. It has the authority to audit organizations, require corrective measures, and sanction entities that fail to protect personal data.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Zimbabwe?

The recently enacted Cyber and Data Protection Act applies to all companies. It imposes obligations on private entities and individuals with respect to privacy and data protection.

2.2 Does privacy law in Zimbabwe apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, the Cyber and Data Protection Act applies to foreign companies if the means used to collect data, whether electronic or otherwise, is located in Zimbabwe, and such processing and storage is not for the purposes of the mere transit of data through Zimbabwe. Where the Act applies to a company outside Zimbabwe, the company is required to designate a representative in Zimbabwe.

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Zimbabwe?

Personal data is referred to as 'Personal Information' in the Cyber and Data Protection Act. 'Personal Information' is defined as including:

- (a) a person's name, address, or telephone number;
- (b) a person's race, national or ethnic origin, color, religious or political beliefs or associations;
- (c) a person's age, sex, sexual orientation, marital status or family status;
- (d) an identifying number, symbol, or other particulars assigned to that person;
- (e) a person's fingerprints, blood type, or inheritable characteristics;
- (f) information about a person's health care history, physical or mental disability;
- (g) information about a person's educational, financial, criminal, or employment history;
- (h) opinions expressed about an identifiable person;
- (i) the individual's personal views or opinions, except if they are about someone else; and
- (j) personal correspondence pertaining to home and family life.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

The Cyber and Data Protection Act states that the following information are ‘sensitive data’:

- (a) information or any opinion about an individual which reveals or contains the following:
 - (i) racial or ethnic origin;
 - (ii) political opinions;
 - (iii) membership of a political association;
 - (iv) religious beliefs or affiliations;
 - (v) philosophical beliefs;
 - (vi) membership of a professional or trade association;
 - (vii) membership of a trade union;
 - (viii) sex life;
 - (ix) criminal educational, financial or employment history; or
 - (x) gender, age, marital status or family status;
- (b) health information about an individual;
- (c) genetic information about an individual; or
- (d) any information which may be considered as presenting a major risk to the rights of the data subject.

Regulations governing sensitive data impose stricter consent requirements, meaning organizations must obtain explicit and informed consent before collecting or processing such information. In certain cases, processing sensitive data is only permitted if it serves a legitimate legal or public interest, such as for healthcare services, national security, or legal proceedings. Additionally, organizations handling sensitive data must implement higher security standards, including encryption, restricted access, and additional safeguards to prevent unauthorized disclosure or breaches.

Sensitive data is also subject to stricter processing limitations, meaning it can only be collected and used for specific, necessary, and legally justified purposes. Unlike general personal data, which may be used for various commercial activities such as marketing, sensitive data is generally prohibited from being processed for profit-driven purposes unless it falls within specific legal exemptions.

Another key distinction is data breach reporting and enforcement. If sensitive personal data is exposed in a data breach, organizations have a heightened duty to report the incident to POTRAZ within a specified timeframe. Failure to comply with these regulations may result in harsher penalties, including significant fines or criminal liability.

Overall, sensitive personal data in Zimbabwe is regulated more strictly than general personal data to ensure that individuals’ privacy and fundamental rights are adequately protected. Businesses and institutions handling such data must implement rigorous compliance measures, including obtaining explicit consent, ensuring lawful processing, and adopting strong security measures to prevent misuse.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

Under the Cyber and Data Protection Act, anonymized, pseudonymized, and de-identified data are treated differently from fully identifiable personal data, but they still fall within the scope of privacy law, depending on how they are used and whether re-identification is possible. Here’s how each type of data is treated under the privacy framework:

- (a) **Anonymized data** refers to personal information that has been processed in such a way that it is no longer possible to identify an individual, either directly or indirectly. When data is fully

anonymized, it no longer falls under the definition of personal data under Zimbabwe's privacy laws. As such, anonymized data is not subject to the same regulatory requirements because it is considered to be outside the scope of the Cyber and Data Protection Act. However, organizations must ensure that the anonymization process is sufficiently rigorous to prevent the possibility of re-identification. If re-identification is possible, even after anonymization, the data would still be considered personal and would be subject to data protection rules.

- (b) **Pseudonymized data** is defined as data that involves replacing identifiable information with pseudonyms or identifiers that cannot directly identify an individual without additional data kept separately. Under Zimbabwean privacy law, pseudonymized data is still considered personal data because re-identification is possible with access to additional information. Therefore, organizations processing pseudonymized data must adhere to the same privacy regulations as for identifiable data. These include obtaining consent from individuals, ensuring data security, and applying data protection measures such as limiting the scope and purpose of data processing. However, pseudonymization can offer some level of protection, reducing the risk of misuse in case of data breaches, as it may lower the likelihood of immediate identification.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

The key obligations for companies under privacy law are:

- (a) to avoid disclosure of sensitive information related to health conditions, children and financial status; and
- (b) where personal data is necessary to know, or limited disclosure required, to seek and obtain advance written consent.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

The Cyber and Data Protection Act defines 'data controller' and 'data processor' differently and assigns different roles to each. The roles affect obligations and contractual requirements:

- (a) the **data controller** is the person or entity which is licensable by the Data Authority, and is the person who determines the purpose and means of data processing;
- (b) the **data processor** does the processing of the data for and on behalf of, and at the instructions of the data controller.

Therefore, the level of responsibility for the data controller is high and obligations under the Cyber and Data Protection Act are imposed primarily on the data controller.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

Zimbabwe's Cyber and Data Protection Act mandates that data controllers have a lawful basis for processing personal data. The Act outlines specific conditions under which personal data can be processed, depending on whether the data is classified as non-sensitive or sensitive:

- (a) Personal information may be processed if the data subject, or a competent person if the data subject is a child, consents to the processing. This consent may be implied if the data subject is an adult with full legal capacity.
Processing is permitted without the data subject's consent if it is necessary for :
 - (i) being material as evidence in proving an offense,
 - (ii) compliance with a legal obligation to which the controller is subject,
 - (iii) protecting the vital interests of the data subject,
 - (iv) performing a task carried out in the public interest or in the exercise of official authority vested in the controller or a third party to whom the data is disclosed, or
 - (v) promoting the legitimate interests of the controller or a third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.
- (b) The Act specifies that sensitive data, which includes information about an individual's race, health, sexual orientation, and other similar categories, requires explicit written consent from the data subject for processing. However, processing without consent is allowed in certain circumstances, such as when necessary:
 - (i) to carry out specific obligations and rights of the controller in the field of employment law,
 - (ii) to protect the vital interests of the data subject or another person when the data subject is incapable of giving consent,
 - (iii) for the establishment, exercise, or defense of legal claims, or
 - (iv) for reasons of substantial public interest,
 among other specified conditions.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

Companies processing personal data for advertising purposes must provide clear privacy notices that include:

- (a) the identity and contact details of the data controller;
- (b) the specific purpose of data collection; and
- (c) information on data subject rights. These rights include:
 - (i) access to their data,
 - (ii) the ability to request corrections or deletions, and
 - (iii) the right to object to the processing of their data for advertising purposes.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

Consumers have several privacy rights concerning their personal data in advertising contexts which include:

- (a) the right to be informed about how their data is used;
- (b) the right to access their collected data;
- (c) the right to request corrections or deletions of inaccurate information; and
- (d) the right to object to the processing of their data for advertising purposes.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

Companies must obtain consent before processing personal data for advertising purposes, especially for direct marketing or targeted ads. They must also provide clear opt-out options, allowing consumers to withdraw consent at any time. Required measures include transparent privacy notices, user-friendly consent mechanisms, and secure systems to manage preferences. Additionally, companies must ensure that data processing aligns with lawful, fair, and proportional principles, protecting consumer rights and preventing unauthorized use of personal information.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

Companies using vendors and third parties for advertising, such as advertising agencies, demand-side platforms ('DSP's), supply-side platforms ('SSP's), or data providers, must ensure that these entities comply with data protection laws. Data controllers remain responsible for how third parties process personal data, and must have contractual agreements outlining data protection obligations, security measures, and restrictions on data use. Transparency is required, meaning consumers must be informed if their data is shared with third parties, and companies must ensure that vendors uphold lawful, fair, and secure data processing practices.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

When disclosing or receiving personal data from vendors or third parties, companies must establish clear contractual obligations to ensure compliance with data protection laws. These contracts must define the purpose and scope of data processing, confidentiality requirements, security measures, data retention policies, and restrictions on further sharing. They must also include clauses ensuring vendors process data lawfully, uphold consumer rights and implement safeguards against unauthorized access or misuse. Additionally, companies should conduct due diligence to verify that third parties adhere to legal and regulatory requirements.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

Companies must undertake due diligence measures, such as verifying third-party compliance with data protection laws, implementing robust security protocols, regularly auditing data processing activities, and ensuring transparency in data collection and usage. They must also provide clear privacy notices and maintain records of data processing activities. Although not required, Impact assessments can be undertaken when advertising uses involve high-risk processing, such as profiling, large-scale data collection, automated decision-making, or the use of sensitive personal data. These assessments help identify potential privacy risks and ensure that appropriate safeguards are in place to protect consumer rights.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

The Cyber and Data Protection Act requires consent for use of personal data; and a consumer has a right, among other things:

- (a) to access their personal information in the custody of a data controller or data processor;
- (b) to object to the processing of all or part of their personal information; and
- (c) to require correction or deletion of false or misleading personal information.

Under the law, complaints can be submitted to POTRAZ.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

The Cyber and Data Protection Act and the Consumer Protection Act may be interpreted as affording protection to consumers in this area.

7.3 How are loyalty programs and promotions regulated under privacy law?

Loyalty programs and promotions are regulated under the Cyber and Data Protection Act.

7.4 How is social media and influencer marketing regulated under privacy law?

Social media and influencer marketing are regulated under privacy law through data protection regulations, requiring informed user consent, transparency in data collection and usage, and compliance with advertising disclosure guidelines to protect consumer privacy.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

Privacy law regulates targeted advertising, including behavioral or personalized advertising, through the Cyber and Data Protection Act, requiring user consent for data collection and processing. By contrast, contextual advertising, which does not rely on personal data tracking, is generally subject to fewer restrictions.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

Digital identity resolution and clean room technologies are regulated under the Cyber and Data Protection Act, which mandates user consent, data minimization, and security measures to protect personal data, ensuring compliance with privacy and confidentiality requirements.

7.7 How is location-based advertising regulated under privacy law?

Location-based advertising is regulated under the Cyber and Data Protection Act, which requires businesses to obtain user consent before collecting, processing, or sharing location data and mandates safeguards to protect individuals' privacy and prevent unauthorized data use.

7.8 How are data brokers defined and regulated under privacy law?

While the Cyber and Data Protection Act does not explicitly define data brokers, it regulates third parties involved in data processing by mandating user consent, enforcing data security measures, and imposing restrictions on the collection, sharing, and use of personal data.

7.9 How is advertising to children and minors regulated under privacy law?

Advertising to children and minors is regulated under the Cyber and Data Protection Act, which mandates parental or guardian consent for processing minors' personal data and imposes restrictions on targeted advertising to protect their privacy and well-being.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

The Cyber and Data Protection Act regulates profiling and the use of artificial intelligence or automated decision-making for advertising by requiring transparency, user consent, and safeguards against unfair or discriminatory data processing practices. The Act specifically provides people with the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

7.11 Are there other specific advertising practices that you wish to discuss?

No.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

Yes, Zimbabwe's privacy law restricts the transfer of personal data across jurisdictions, allowing it only if the recipient country or international organization ensures an adequate level of data protection. The law requires that data transfers be assessed based on factors such as the recipient's data protection laws, security measures, and professional standards, and, in cases where adequate protection is not ensured, transfers may only occur under specific conditions such as obtaining the data subject's consent or fulfilling contractual obligations. POTRAZ has the power to determine categories of processing operations and circumstances in which data transfers to certain countries are not authorized, but no specific prohibited jurisdictions are explicitly listed in the provided text.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

Additional considerations for personal data transfers in Zimbabwe include legal and public interest requirements, the protection of the data subject's vital interests, and the need for compliance with laws governing public registers accessible to those with a legitimate interest.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Zimbabwe? Are there minimum standards? Does this differ by sector or size of the entity?

The Cyber and Data Protection Act requires the data controller or its representative to take the appropriate technical and organizational measures that are necessary to protect the security, integrity and confidentiality of the data. The data processed must be protected from negligent or unauthorized

destruction, negligent loss, unauthorized alteration or access, and any other unauthorized processing of the data.

There are no official resources available to help companies address this standard. POTRAZ may, however, in due course provide information and guidance on compliance.

9.2 How are personal data breaches regulated in Zimbabwe? What are the requirements for notification and response?

The Cyber and Data Protection Act provides for POTRAZ to be established under the Post and Telecommunications Authority. There is an obligation for companies to provide notifications to POTRAZ whenever there is a data breach.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

Penalties and/or sanctions, as well as damages, will be determined by the specific law under which the violation or breach of privacy occurred; and may be determined/imposed through arbitration or a court of law.

10.2 Do consumers have a private right of action? What remedies are available to them?

Depending upon the circumstances, there may be a private right of action at POTRAZ, in court; and damages as well as an interdict may be granted.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

The Cyber and Data Protection Act was only recently enacted (in 2021). Thus far there have not been any enforcement actions or lawsuits.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Zimbabwe?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

Artificial intelligence ('AI') is a hot topic for many reasons including its potential use to disrupt privacy.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

Greater awareness of the value and use of data, mainly due to increased use of social media and mobile applications for sales and marketing.

Consistent with its adoption of the African Union Convention on Cyber Security and Personal Data Protection in June 2014, Zimbabwe enacted the Cyber and Data Protection Act in December 2021.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

Increasing regulations will require considerable financial resources and administrative time. It will be difficult for businesses, particularly those which are newly established, to be able to afford the additional costs and sustain a viable business.

12.3 What do you envision the privacy landscape will look like in five years?

The global trend requires electronic commerce for economies to keep afloat. There will be large amounts of personal data being used by the government and private sector, not only within, but outside Zimbabwe. Cases of identity theft and fraud are set to be on the rise as personal information becomes easy to access, resulting in the necessity for regulatory controls and restrictions on access and use.



LIST OF GALA MEMBERS



ALGERIA

Dina Eldib & Mohamed Eldib
Eldib & Co
 Citadel Plaza Building 1, Intersection
 Of Mokattam Road & Autostrade,
 Mokattam, Cairo 11411
 T: +20.2.2510.2222
 E: mohamed.eldib@eldib.com
 E: dina.eldib@eldib.com
 W: www.eldib.com

ARGENTINA

Dámaso Pardo & Franco Raffinetti
Bruchou & Funes de Rioja
 Ing. Enrique Butty 275, 12th Floor
 Buenos Aires C1001AFA
 T: +54.11. 4021.2300
 E: Damaso.pardo@bruchoufunes.com
 E: Franco.raffinetti@bruchoufunes.com
 W: www.bruchoufunes.com

AUSTRALIA

Peter Le Guay & Bronwyn Furse
Thomson Geer
 Level 14, 60 Martin Place
 Sydney NSW 2000
 T: +61.2.8248.5800
 E: pleguay@tglaw.com.au
 E: bfurse@tglaw.com.au
 W: www.tglaw.com.au

AUSTRIA

Stefan Kofler & Georg Huber
GPK Pegger Kofler & Partner
Rechtsanwälte GmbH & Co KG
 Maria-Theresia Strasse 24,
 A-6020 Innsbruck
 T: +43.512.571.811
 E: stefan.kofler@lawfirm.at
 E: georg.huber@lawfirm.at
 W: www.lawfirm.at

BELGIUM

Jan Ravelingien
Marx, Van Ranst, Vermeersch
& Partners
 Avenue de Tervueren 270,
 1150 Brussels
 T: +32.2.285.01.00
 E: jan.ravelingien@mvvp.be
 W: www.mvvp.be

BOLIVIA

Ramiro Moreno Baldivieso &
 Rodrigo Moreno
Moreno Baldivieso
 Torre Pacifico, Piso 8, Av. Sánchez
 Bustamante No. 977, esq. Calle 16,
 Calacoto, La Paz
 T: +591.2. 2791554
 E: morenob@emba.com.bo
 E: rmorenog@emba.com.bo
 W: www.emba.com.bo

BOSNIA & HERZEGOVINA

Mirna Milanović-Lalić & Jasmina Suljović
Law Office Milanović-Lalić and Suljović
 Gabelina 2, Sarajevo 71000
 T: + 387.33.558.565
 E: mirna@bh.legal
 E: jasmina@bh.legal
 W: www.bh.legal

BRAZIL

Valdir Rocha & Roberta Medina
Veirano Advogados
 Av. Bartolomeu Mitre, 770 – Leblon
 CEP: 22431-004 - Rio de Janeiro/RJ
 T: +55 21 3824-4747
 E: valdir.rocha@veirano.com.br
 E: roberta.medina@veirano.com.br
 W: www.veirano.com.br

BULGARIA

Violetta Kunze & Ralitsa Gougleva
Djingov, Gouginski, Kyutchukov & Velichkov
 10 Tsar Osvoboditel Blvd.
 Sofia 1000
 T: +359.2.932.1100
 E: violetta.kunze@dgkv.com
 E: ralitsa.gougleva@dgkv.com
 E: dgkv@dgkv.com
 W: www.dgkv.com

CANADA

Catherine Dennis Brooks
 & Jaclyne Reive
Miller Thomson LLP
 Scotia Plaza, 40 King Street West, Suite
 6600, Toronto, Ontario, M5H 3S1
 T: 416.595.8567
 T: 416.595.7935
 E: cdennisbrooks@millerthomson.com
 E: jreive@millerthomson.com
 W: www.millerthomson.com

CANADA (cont'd)

Kelly Harris & Lauren Shrubbs
Harris + co.
 221-451 Dundas St W
 Toronto M5T 1G8
 T: 647.632.2907
 E: kellyharris@harrisandco.ca
 E: laurenshrubbs@harrisandco.ca
 W: www.harrisandco.ca

CARIBBEAN

Karyl D. Bertrand (Dutch)
Bertrand Legal
 Castorweg 22-24
 Willemstad, Curaçao
 T: +5999 461 8183
 E: karyl@bertrand-legal.com

Dianne Daley & Marissa Longworth
 (English)
Foga Daley
 7 Stanton Terrace, Kingston 6,
 St. Andrew, Jamaica
 T: +876 927 4371
 E: daley@fogadaley.com
 E: marissa@marissalongworth.com
 W: www.fogadaley.com

CHILE

Ariela Agosin & Eugenio Gormáz
Albagli Zaliasnik
 Av. El Golf 150, Piso 4, Las Condes
 Santiago
 T: +56 2 2 445 6000
 E: aagosin@az.cl
 E: egormaz@az.cl
 W: www.az.cl

CHINA

Philip Qu & Eric Johnson
TransAsia Lawyers
 Suite 2218, China World Office 1,
 1 Jianguomenwai Avenue,
 Beijing 100004
 T: +86 10 6505 8188
 E: pqu@TransAsiaLawyers.com
 E: ejohnson@TransAsiaLawyers.com
 W: www.TransAsiaLawyers.com

COLOMBIA

Juan Carlos Uribe & Sandra Ávila
Triana, Uribe & Michelsen
 Calle 93B No. 12-48 P. 4,
 Bogotá, D.C. 110221
 T: +57 1 6019660
 E: jcu@tumnet.com
 E: sag@tumnet.com
 W: www.tumnet.com

COSTA RICA

Uri Weinstok M. & Leon Weinstok
BLP
 BLP Building, 4th floor. Via Lindora
 Business Center, San Jose
 T: +506.2205.3939
 E: uweinstok@blplegal.com
 E: lweinstok@blplegal.com
 W: www.blplegal.com

CROATIA

Mladen Vukmir
Vukmir & Associates
 Gramaca 2L 10 000 Zagreb
 T: +385.1.376.0511
 E: mladen.vukmir@vukmir.net
 W: www.vukmir.net

CYPRUS

Polina Christodoulo &
 Vasilis Charalambous
George Z. Georgiou & Associates LLC
 1 Iras Street, Nicosia 1060
 T: +35722763340
 E: polina.christodoulo@gzg.com.cy
 E: vasilis.charalambous@gzg.com.cy
 W: www.gzg.com.cy

CZECH REPUBLIC

Irena Lišková, Ladislav Mádl,
 & Eliska Rihova
Randl Partners
 Budějovická 1550/15a
 Praha 4 140 00
 T: +420 222 755 311
 E: liskova@randls.com
 E: madl@randls.com
 E: rihova@randls.com
 W: www.randls.com

DENMARK

Johan Løje
Løje IP
 Øster Allé 42, 6. floor
 DK-2100 Copenhagen
 T: + 45 32 42 05 41
 E: jl@loje-ip.dk
 W: www.loje-ip.dk

DOMINICAN REPUBLIC

Jaime R. Angeles
AngelesPons
 Ave. Roberto Pastoriza No. 412,
 Edificio Altri Tempi, Suite 501, Piantini,
 Santo Domingo, D.N.
 T: +809.373.9418
 E: jangeles@angelespons.com
 W: www.angelespons.com

ECUADOR

Jaime Mantilla, Alexander Orozco
 & Carlos Alberto Arroyo Del Río
Falconi Puig Abogados
 Av. Amazonas N21-147 y Roca
 Edificio Río Amazonas,
 Oficina 900, Quito
 T: +593.2. 256.1808
 E: jmantilla@falconipuig.com
 E: aorozco@falconipuig.com
 E: carroyodelrio@falconipuig.com
 W: www.falconipuig.com

EGYPT

Dina Eldib & Mohamed Eldib
Eldib & Co
 Citadel Plaza Building 1, Intersection
 Of Mokattam Road & Autostrade,
 Mokattam, Cairo 11411
 T: +20.2.2510.2222
 E: mohamed.eldib@eldib.com
 E: dina.eldib@eldib.com
 W: www.eldib.com

EL SALVADOR

Marcela Mancia
IDEAS Trademarks & Patents
 Avenida Las Palmas #183, Colonia
 San Benito, San Salvador
 T: +503.2566.5260
 E: mmancia@ideasips.com
 W: www.ideasips.com

ESTONIA

Egon Talur
COBALT
 Kawe Plaza, Pärnu mnt 15, Tallinn 10141
 T: + 372.665.1888
 E: egon.talur@cobalt.legal
 W: www.cobalt.legal

FINLAND

Mikael Segercrantz &
 Johanna Lilja
Roschier, Attorneys Ltd.
 Kasarmikatu 21A, Helsinki 00130
 T: + 358.20.506.6000
 E: mikael.segercrantz@roschier.com
 E: johanna.lilja@roschier.com
 W: www.roschier.com

FRANCE

Caroline Bouvier
Bernard Hertz Béjot
 1 rue de Chazelles – 75017 Paris
 T: +33.1.43.18.8080
 E: cbouvier@bhbfrance.com
 W: www.bhbfrance.com

GERMANY

Søren Pietzcker (Hamburg Office),
 Dominik Eickemeier (Cologne Office),
 Thorsten Wieland (Frankfurt Office), & Philip
 Kepermann (Dusseldorf Office)
Heuking Kühn Lüer Wojtek
 Neuer Wall 63, Hamburg
 T: +49.40.355.280.53
 E: s.pietzcker@heuking.de
 E: d.eickemeier@heuking.de
 E: p.kepermann@heuking.de
 E: t.wieland@heuking.de
 W: www.heuking.de

GHANA

Olusola Ogundimu & Esohe Olajide
Integrated Legal Consultants
 12, Nii Amaah Ollenu Street, Airport West
 GA-193-5159, P.M.B. 52, Kanda, Accra
 T: +233 302 770 496
 E: olusola@integratedlegalconsultants.com
 E: esohe@integratedlegalconsultants.com
 W: www.integratedlegalconsultants.com

GREECE

Kriton Metaxopoulos
A. & K. Metaxopoulos & Partners
Law Firm
 54 Vas. Sofias Av. , 11528 Athens
 T: +30.210.7257614
 E: k.metaxopoulos@metaxopouloslaw.gr
 W: www.metaxopouloslaw.gr

GUATEMALA

Marco Antonio Palacios & Diego Palacios
Palacios Abogados
 Diagonal 6, 12-42, Zona 10,
 Edificio Design Center, Torre I, Nivel 3,
 Oficina 30, Guatemala City
 T: +502.2231.8500
 E: mapalacios@sercomi.com.gt
 E: dpalacios@sercomi.com.gt
 W: www.palacios.com.gt

HONDURAS

José M. Álvarez & Fernando Godoy
BLP
 Torre BLP, 7mo nivel, Colonia
 Matamoros, Calle Venecia,
 No. 2423, Tegucigalpa
 T: 504 2269 1217
 E: jalvarez@blplegal.com
 E: fgodoy@blplegal.com
 W: www.blplegal.com

HONG KONG

Anthony Leung & John McLellan
Haldanes
 7th Floor, Ruttonjee House,
 11 Duddell Street, Central
 T: +852.2868.1234
 E: Anthony.leung@haldanes.com
 E: jpm@haldanes.com
 W: www.haldanes.com

HUNGARY

Anikó Keller, Zoltán Kovács,
 & Gábor Faludi Jr.
Szecskey Attorneys at Law
 H-1055 Budapest, Kossuth Lajos
 tér 16-17
 T: +36 1 472 3000
 E: aniko.keller@szecskey.com
 E: zoltan.kovacs@szecskey.com
 E: gabor.faludi.jr@szecskey.com
 W: www.szecskey.com

INDIA

Sharad Vadehra
Kan and Krishme
 KNK House, A-11 Shubham Enclave
 Paschim Vihar, New Delhi-110063
 T: +91.11.4377 66 66
 E: knk@kankrishme.com
 E: vadehra666@gmail.com
 W: www.kankrishme.com

IRELAND

Conor Griffin
Duncan Grehan & Partners Solicitors
 26 Fitzwilliam Street Upper, Dublin 2
 T: +353.1677.9078
 E: cgriffin@duncangrehan.com
 W: www.duncangrehan.com

ISRAEL

David Wolberg
Kuperschmit, Goldstein & Co.
 Kefar Netter Industrial Park,
 P.O. Box 3726, Kefar Netter 4059300
 T: +972.9.835.6122
 E: dwolberg@kgcolaw.co.il
 W: www.kgcolaw.co.il

ITALY

Laura Liguori & Eleonora Curreli
Portolano Cavallo
 Via Rasella 155
 Rome 00187
 T: + 39.06.696.661
 E: lliguori@portolano.it
 E: ecurreli@portolano.it
 W: www.portolano.it

JAPAN

Chie Kasahara
Atsumi & Sakai
 Fukoku Seimei Bldg.,
 Reception: 16th Floor
 2-2-2 Uchisaiwaicho, Chiyoda-ku,
 Tokyo 100-0011
 T: +81 3-5501-2438 (Direct)
 E: chie.kasahara@aplav.jp
 W: www.aplav.jp/en/

KENYA

John Syekei, Daniel Mwathe
 & Ariana Issaias
Bowmans Kenya
 5th Floor, ICEA Lion Centre,
 Riverside Park, Chiromo Road
 Nairobi
 T: +254 20 289 9000
 E: john.syekei@bowmanslaw.com
 E: daniel.mwathe@bowmanslaw.com
 E: ariana.issaias@bowmanslaw.com
 W: www.bowmanslaw.com

LATVIA

Indrikis Liepa & Gabriela Santare
Cobalt
 Marijas iela 13 k-2, Riga 1050
 T: + 371.6720.1800
 E: Indrikis.liepa@cobalt.legal
 E: gabriela.santare@cobalt.legal
 W: www.cobalt.legal

LITHUANIA

Renata Vasiliauskiene
Cobalt
 Lvovo 25, Vilnius 09320
 T: + 370.5250.0800
 E: renata.vasiliauskiene@cobalt.legal
 W: www.cobalt.legal

LUXEMBOURG

Michel Molitor & Virginie Liebermann
MOLITOR Avocats à la Cour
 8, rue Sainte - Zithe, B.P.690, L-2016
 T: +352.297.298/1
 E: michel.molitor@molitorlegal.lu
 E: virginie.liebermann@molitorlegal.lu
 W: www.molitorlegal.lu

MALAYSIA

Patrick Mirandah
Mirandah Asia
 Suite 3B-19-3 Plaza Sentral, Jalan
 Stesen Sentral 5, 50470 Kuala Lumpur
 T: +603.2278 86 86
 E: malaysia@mirandah.com
 W: www.mirandah.com

MALTA

Kris Scicluna
Aequitas Legal
 Valletta Buildings, South Street
 Valletta, 1103
 T: +356 21 234085
 E: kscicluna@aequitas.com.mt
 W: www.aequitas.com.mt

MEXICO

Roberto Arochi, José Antonio Arochi,
 Veronica Siten, & Gabriela Espinosa
Arochi & Lindner
 Insurgentes Sur 1605, 20th Floor
 San José Insurgentes, Mexico City,
 03900
 T: +52.55.50.95.2050
 E: rarochi@arochilindner.com
 E: jarochi@arochilindner.com
 E: vsiten@arochilindner.com
 E: gspinoso@arochilindner.com
 W: www.arochilindner.com

MOROCCO

Dina Eldib & Mohamed Eldib
Eldib & Co
 Citadel Plaza Building 1, Intersection
 Of Mokattam Road & Autostrade,
 Mokattam, Cairo 11411
 T: +20.2.2510.2222
 E: mohamed.eldib@eldib.com
 E: dina.eldib@eldib.com
 W: www.eldib.com

NETHERLANDS

Lisa Peek, Luna Snellenberg
 & Daniël Haije
Hoogenraad & Haak
 Cruquiusweg 109-B, 1019 AG
 Amsterdam
 T: +31 20 305 3066
 E: lisa.peek@hoogenhaak.nl
 E: luna.snellenberg@hoogenhaak.nl
 E: dh@hoogenhaak.nl
 W: www.hoogenhaak.nl

NEW ZEALAND

Erich Bachmann &
 Julika Wahlmann-Smith
Hesketh Henry
 Level 14, 188 Quay Street,
 Auckland 1010
 T: +64.9.375.8709
 E: erich.bachmann@heskethhenry.co.nz
 E: julika.wahlmann-smith@heskethhenry.co.nz
 W: www.heskethhenry.co.nz

NICARAGUA

Julián J. Bendaña-Aragón &
 Ana Jeanssy Fornos
Guy José Bendaña-Guerrero
 & Asociados
 PO Box 3140, Managua 00005
 T: +505.2266.5662
 E: julian.bendana@guybendana.com.ni
 W: www.guybendana.com.ni

NIGERIA

Lara Kayode & Dozie Ezech
O. Kayode & Co.
 21 Olanrewaju Street Of Billingsway
 Oregun Lagos
 T: +234 1 291 2412
 E: lara@okayode.com
 E: dozie@okayode.com
 W: www.okayode.com

NORTH MACEDONIA

Aleksandar Kchev
Bona Fide Law Firm
 Jordan Hadzikonstantinov-Dzinot 3,
 kopje, 1000
 T: +389(2)3.23.2. 65
 E: akcev@bonafide.mk
 W: www.bonafide.mk

NORWAY

Rune Nordengen
Advokatfirmaet Bull AS
 PO Box 6604 St. Olavs Plass,
 0129 Oslo
 T: +47.23.01.01.01
 E: rn@bull.no
 W: www.bullco.no

PANAMA

Ramón R Benedetti A. & Chris Effio
Estudio Benedetti
 Samuel Lewis Avenue, Comosa Building,
 19th Floor, PO Box 823-00183
 T: + 507.321.5100
 E: ramon@estudiobenedetti.com
 E: ceffio@estudiobenedetti.com
 W: www.estudiobenedetti.com

PARAGUAY

Hugo Mersan, Lorena Mersan
 & Liliana Nolan
MERSAN
 Fulgencio R. Moreno No. 509 –
 Edificio De La Colina 3° Piso
 Casilla de Correos 693 – Asunción
 T: + 595 21 447 739
 E: hugo@mersanlaw.com
 E: lorenamersan@mersanlaw.com
 E: liliananolan@mersanlaw.com
 W: www.mersanlaw.com

PERU

Jorge Allende
Allende & Garcia Abogados
 Av. del Pinar 180 Of. 504,
 Chacarilla, Lima 33
 T: + 51 1 372 0395
 E: jorge@allendegarcia.com.pe
 W: www.allendegarcia.com.pe

POLAND

Jacek Myszko, Agata Szeliga
 & Sandra Słowik
Softysinski Kawecki & Szlezak
Legal Advisors
 ul. Jasna 26, 00-054 Warsaw
 T: +48.22.608.70.47
 E: Jacek.Myszko@sklegal.pl
 W: www.sklegal.pl

PORTUGAL

César Bessa Monteiro &
 Ricardo Henriques
Abreu Advogados
 Av. Infante D. Henrique, 26
 Lisbon 1149-096
 T: +351. 217 231 800
 E: bessa.monteiro@abreuadvogados.com
 E: ricardo.henriques@abreuadvogados.com
 W: www.abreuadvogados.com

PUERTO RICO

Eugenio Torres
Ferraiuoli LLC
 221 Ponce de León Avenue, 5th Floor
 Hato Rey, Puerto Rico 00917
 T: 787.766.7000
 E: etorres@ferraiuoli.com
 W: www.ferraiuoli.com

ROMANIA

Elena Stan
Stratulat Albulescu Attorneys at Law
 One Herastrau Office
 30-32 Daniel Danielopolu Street,
 District 1, Bucharest, 014134
 T: 40.21.316.87.49
 E: estan@saa.ro
 W: www.saa.ro

RWANDA

Brenda Vilita & Lorna Mbatia
CFL Advocates
 Building KG 11 AV 10, 2nd Floor,
 Gisimenti Kigali
 T: 250.787.595.925
 E: brenda@cfllegal.com
 E: lorna@cfllegal.com
 W: www.cfllegal.com

SERBIA

Slobodan Kremenjak, Nebojša
 Samardžić & Kruna Savović
Živković Samardžić
 Makedonska 30/II
 Belgrade 11000
 T: + 381 11 2636636
 E: slobodan.kremenjak@zslaw.rs
 E: nebojsa.samardzic@zslaw.rs
 E: kruna.savovic@zslaw.rs
 W: www.zslaw.rs

SINGAPORE

Denise Mirandah
Mirandah Asia
 1 Coleman Street, #07 - 08
 The Adelphi, 179803
 T: +65.63369696
 E: denise@mirandah.com
 W: www.mirandah.com

SLOVAKIA

Peter Marciš & Marek Bugan
Nitschneider & Partners
 Lazaretská 12, 811 08 Bratislava
 T: +421 2 2092 1213
 E: marcis@nitschneider.com
 E: bugan@nitschneider.com
 W: www.nitschneider.com

SOUTH AFRICA

Kelly Thompson, Jenny Pienaar,
 & Mercia Fynn
Adams & Adams
 P O Box 1014, Pretoria, 0001
 T: +27 12 432 6000
 E: kelly.thompson@adams.africa
 E: jenny.pienaar@adams.africa
 E: mercia.fynn@adams.africa
 W: www.adams.africa

SOUTH KOREA

Chunghwan Choi, Yong Min Lee,
 & Doil Son
Yulchon
 Parnas Tower, 38F, 521 Teheran-ro,
 Gangnam-gu, Seoul
 06164
 T: +82.2.528.5200
 E: chchoi@yulchon.com
 E: ymlee@yulchon.com
 E: dison@yulchon.com
 W: www.yulchon.com

SPAIN

Ignacio Temiño Cenicerós
 & Salvador Diaz
Abril Abogados
 Calle Zurbano, 76
 Madrid 28010
 T: +34 91 7020331
 E: ignaciot@abrilabogados.com
 E: sdiaz@abrilabogados.com
 W: www.abrilabogados.com

SWEDEN

Richard Wessman
Advokatfirman Vinge KB
 Smålandsgatan 20, Box 1703,
 Stockholm, 111 87
 T: + 46 (0)70 886 04 04
 E: Richard.Wessman@vinge.se
 W: www.vinge.se/en

SWITZERLAND

Dr. Rolf Auf der Maur, Sarah Bischof,
 & Sefora Pileggi
VISCHER AG
 Schuetzengasse 1, P.O. Box,
 CH-8021 Zurich
 T: +41 58 211 34 00
 E: ram@vischer.com
 E: sarah.bischof@vischer.com
 E: sefora.pileggi@vischer.com
 W: www.vischer.com

TRINIDAD AND TOBAGO

Stephanie Moe
*Fitzwilliam Stone Furness-
 Smith & Morgan*
 48-50 Sackville Street
 Port of Spain
 T: +868.623.1618
 E: smoe@fitzwilliamstone.com
 W: www.fitzwilliamstone.com

TURKEY

Ugur Aktekin, Begüm Yavuzdoğan
 Okumuş, & Yalçın Umut Talay
Gün + Partners Avukatlık Bürosu
 Kore Sehitleri Cad. No: 17,
 Zincirlikuyu 34394, Istanbul
 T: +90.212.3540000
 E: ugur.aktekin@gun.av.tr
 E: begum.yavuzdogan@gun.av.tr
 E: umut.talay@gun.av.tr
 W: www.gun.av.tr

TUNISIA

Dina Eldib & Mohamed Eldib
Eldib & Co
 Citadel Plaza Building 1, Intersection
 Of Mokattam Road & Autostrade,
 Mokattam, Cairo 11411
 T: +20.2.2510.2222
 E: mohamed.eldib@eldib.com
 E: dina.eldib@eldib.com
 W: www.eldib.com

UGANDA

Paul Asiimwe & Bridget Mategyero
Sipi Law Associates
 Jocasa House, Unit 5, 3rd Floor
 Plot 14 Nakasero Rd, #4180, Kampala
 T: +256.414.235391/312.272921
 E: paul@sipilawuganda.com
 E: bridget@sipilawuganda.com
 W: www.sipilawuganda.com

UKRAINE

Oleg Klymchuk, Anastasiia Finko,
& Viktoriia Posvystak.
Sayenko Kharenko
10 Muzeyny Provulok,
Kyiv 01001
T: +380 44 499 6000
E: OKlymchuk@sk.ua
E: AFinko@sk.ua
E: VPosvystak@sk.ua
W: www.sk.ua

UNITED KINGDOM

Brinsley Dresden, Bryony Long,
& Mark Hersey
Lewis Silkin LLP
5 Chancery Lane, Clifford's Inn,
London EC4A 1BL
T: +44 (0) 20.7074.8069
E: brinsley.dresden@lewissilkin.com
E: bryony.long@lewissilkin.com
E: mark.hersey@lewissilkin.com
W: www.lewissilkin.com

UNITED STATES OF AMERICA

Ronald R. Urbach & Allison Fitzpatrick
Davis+Gilbert LLP
1675 Broadway, New York, NY 10019
T: +1.212.468.4800
E: rurbach@dglaw.com
E: afitzpatrick@dglaw.com
W: www.dglaw.com

Daniel Goldberg, Jeffrey A. Greenbaum,
& Andrew Folks
Frankfurt Kurnit Klein & Selz P.C.
28 Liberty Street,
New York, New York 10005
T: +1.212.980.0120
E: dgoldberg@fkks.com
E: jgreenbaum@fkks.com
E: afolks@fkks.com
W: www.fkks.com

UNITED STATES OF AMERICA (cont'd)

Melissa Landau Steinman & Milo Cividanes
Venable LLP
600 Massachusetts Avenue NW
Washington D.C. 20001
T: +1 202 344 4000
E: mlsteinman@venable.com
E: ecividanes@Venable.com
W: www.venable.com

URUGUAY

Alejandro Alterwain & Martín Pesce
Ferrere
Juncal 1392, Ferrere Tower,
11.000 Montevideo
T: +598 2 900 1000
E: aalterwain@ferrere.com
E: mpesce@ferrere.com
W: www.ferrere.com

VENEZUELA

Ricardo Alberto Antequera
Antequera Parilli & Rodriguez
Edificio Centro COINASA, PH-B, Avenida
San Felipe, La Castellana, Caracas 1060
T: +58.212.263.9944
E: ricardoalberto@antequera.legal
W: www.antequera.com.ve

ZIMBABWE

Brenda M. Wood Kahari
B.W. Kahari
Baronage House, 24 Lanark Road
Belgravia/Avondale, Harare
T: +263.242.250994/5 or 253941
E: brendak@bwkahari.com
W: www.lawyersforafrica.com



28 Liberty Street, 35th Floor, New York, NY 10005

Tel: 212.705.4895 | Fax: 347.438.2185 | Email: sbess@galalaw.com

www.galalaw.com