GALA
GLOBAL ADVERTISING LAWYERS ALLIANCE

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

Published in Cooperation with the IAA
INTERNATIONAL ADVERTISING ASSOCIATION

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

FOREWORD

Advertising has changed dramatically over the past decade. Rapid developments in technology, the proliferation of social media, and increased access to consumer data have allowed publishers, brands, agencies, and other players in the advertising ecosystem to better understand consumers and deliver more relevant content. Consumer data is incredibly valuable and can be used for purposes such as research and analysis, calculating attribution for campaigns, email and text marketing, delivering personalized advertising, and finding prospective customers in ways not previously possible. For example, a brand can upload its customer list to a social media platform, and serve advertising on the platform to both customers on that list as well as segments of customers identified by the platform as similar to the brand's customers and likely to purchase the brand's products.

The increased reliance on consumer data has led to inevitable questions about the need for regulation over consumer privacy. While privacy is not a new concept, privacy exploded on a global scale in 2018 due to a combination of factors. Most significantly, the European Union began enforcing its robust data protection law, the General Data Protection Regulation (GDPR), which gave regulators the ability to issue dramatic penalties against companies for improperly processing data about individuals located in Europe. Concerned about the ease of data flows across borders and the growing importance of international markets, companies around the world took measures to address the obligations of the GPDR. At the same time, the world learned about the Facebook-Cambridge Analytica incident, which created heightened awareness of the power of data and the potential for misuse.

Privacy compliance has shifted from a business best practice to a business necessity. Since 2018, numerous jurisdictions have updated their privacy laws to bring them closer to GDPR standards. For instance, California and Brazil both passed GDPR-like privacy laws, effective in 2020. While many of the new laws share similarities to the GDPR, they differ in key aspects and require independent analysis. Companies must now understand the

nuances between privacy obligations in their home jurisdictions and those elsewhere, and implement procedures and systems to harmonize compliance.

This book, developed by the Global Advertising Alliance (GALA), in cooperation with the International Advertising Association (IAA), is the first, to our knowledge, designed specifically to address global privacy laws in the context of the advertising ecosystem. GALA members across 70 countries with expertise in privacy in their respective jurisdictions helped develop the content for the book. Each chapter covers a specific country, giving a background on the privacy framework for that country, detailing key issues in relation to advertising, and concluding with opinions from the author of that chapter as to the state of privacy in that country. To improve readability of the book, GALA divided the book into two parts. Part one focuses on countries outside the European Union, while part two starts with an overview of the GDPR and then focuses on countries within the European Union that are subject to the GDPR. The digital version of the book includes both parts.

While there are great differences in the ways that privacy is addressed around the world, there are certainly some key trends across jurisdictions:

- Countries are more focused than ever before on privacy, and many are developing robust laws with harsh penalties. However, compliance can be difficult because laws often are not technologically agnostic and struggle to fit advancements in technology.

- The types of consumer data considered to be personally identifiable have broadened substantially. Information previously treated by the advertising ecosystem as "de-identified" or "anonymous," such as IP addresses and Ad IDs, could fall within scope of privacy laws.

- Transparency and choice are becoming universal concepts. Privacy laws around the world accept the notion that consumers have the right to know what information is being collected from them and the purposes for which it is being collected. They also frequently give consumers the right to limit use of their information for marketing purposes. Depending on the jurisdiction and other factors, choice may require opt-in or opt-out consent.

- Practices that are not specifically prohibited by law could still violate the law or create public relations issues if those practices do not meet the reasonable expectations of consumers. Providing better notice to consumers and avoiding "creepy" practices can help address potential issues.

- In response to globalization, some countries have instituted strict data localization requirements. Cross-border data flows require additional consideration.

- Global data security and breach response obligations have dramatically evolved over the past decade, playing catch up to those already found under U.S. law. Violations often carry harsh penalties.

- Privacy regulation comes not just from lawmakers, but also from the platforms and browsers from which data is collected. Changes to their policies and technology have a fundamental impact on the advertising ecosystem and privacy compliance efforts.

- Profiling and automated decision-making carry increased scrutiny. Many jurisdictions impose specific obligations, such as internal assessments, around related data processing.

- Jurisdictions do not always align on balancing privacy, surveillance, and freedom of speech. Companies should aim to understand local belief systems and practices when processing data about consumers related to that jurisdiction.

It is important to note that this book reflects a snapshot in time and was developed prior to the COVID-19 pandemic of 2020. As such, the content does not address the impact of COVID-19 on privacy law. Countries around the world have taken measures to combat COVID-19, including through development of apps designed to trace the spread of COVID-19 that rely on the processing of vast amounts of consumer data. These measures may have a short term impact on privacy rights and expectations, and could ultimately result in long term increased privacy regulation as consumers become more concerned

about how their data is used. We reserve discussion of the impact of COVID-19 for the next edition of this book.

A big thank you to all of the GALA members who contributed to this book, as well as to the IAA for its collaboration efforts. This book would not be possible without all their hard work. Special thank you to Stacy Bess (Executive Director of GALA), Jeff Greenbaum (Chairman of GALA), Søren Pietzcker (who led writing of the GDPR chapter of the book), Srinivasan Swamy (Chairman & World President of IAA), Carla Michelotti (Global VP of Government Affairs of IAA), and Dagmara Szulce (Managing Director of IAA).

On behalf of GALA, we appreciate you choosing to read our book, and hope you find it to be a valuable resource.

Daniel Goldberg
Frankfurt Kurnit Klein & Selz, PC

May 15, 2020

INTRODUCTION

For over eight decades, the International Advertising Association (IAA) has played a significant role globally identifying and educating marketing and advertising thought leadership about key industry issues by promoting and defending freedom of commercial speech; establishing and supporting effective and meaningful advertising industry self-regulation; defending the value of brands, and their important role in consumer choice; and in the digital world encouraging respect for consumer privacy while promoting the growth of digital commerce and communication.

In April 2019, some of IAA Board members called on Jeffrey A. Greenbaum, Chairman of the Global Advertising Lawyers Alliance (GALA) and also the Managing Partner of Frankfurt Kurnit Klein & Selz PC in his New York office to discuss privacy and the current digital environment.

In the course of the discussions, we talked about the digital privacy issues that are raging in different parts of the world and how governments are coming up with a wide variety of laws to protect their people. We also talked about how difficult it was for businesses to navigate the landscape of different, and ever-changing, rules – and that they needed additional resources they could turn to, for reference. Jeff promptly agreed that through its extensive network of lawyers in various countries, GALA is well equipped to put together a handbook on the multiplicity of privacy laws that impacts advertising and marketing. This, we felt, would be a much-needed compendium. It would be an important resource for large companies who are operating in different geographies to turn to, with communication seamlessly flowing across borders.

Over the last several months, GALA's members from around the world have distilled the details of the privacy laws impacting advertising and marketing in more than 70 countries, providing critical information about the laws and regulations that protect persons consuming digital media and those who are targeted by digital marketing.

We hope that this Global Privacy Laws handbook will be an excellent reference volume to all major marketing companies and governments around the world. The book demonstrates how some countries have simple laws that are easy to follow and how some countries have made the laws quite complex.

IAA invited GALA to become an institutional member and take on a Board position at IAA. The association between the two global institutions could gain from each other, as both serve the interest of Marcom practitioners. IAA believes that its promise of being Global Compass for Marketing Communications is consistent with GALA's view.

We do know that this professional labor of love by GALA lawyers is a welcome addition to many law books that are available in the world. IAA is indeed delighted to have been associated in bringing out this landmark book for the benefit of the industry.

We thank the GALA team for the enormous effort and thought leadership that went into creating this valuable global resource.

Srinivasan K. Swamy
IAA Chairman & World President

June 3, 2020

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

ARGENTINA

1 PRIVACY LAW

1.1 How is privacy 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 (Section 1770) 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. Moreover, in 2003, the European Union issued a resolution establishing that Argentina had a level of protection consistent with the protection granted by the Data Protection Directive 95/46/EC with respect to personal data.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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;

(c) Provisions issued by the National Directorate of Data Protection ("DPND");

(d) PDPA-Disposition No 4/2004, approving the Ethic Code of the Association of Direct and Interactive Marketing ("AMDIA");

(e) Law No 26,951 (the "Do-Not-Call Law"), creating the "Do-Not-Call Registry" and expanding the protection of data owners' rights. This regulation allows a data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephonic means must register with the Agency and consult the list of blocked numbers on a monthly basis before engaging in marketing calls. Furthermore, Law No 2,014 of the City of Buenos Aires and Law No 14,326 of the Province of Buenos Aires have created their own do-not-call registries, within their jurisdiction;

(f) PDPA-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;

(g) PDPA-Disposition 20/2015, regulating the collection of photos, films, sounds or any other data in digital format through unmanned aerial vehicles or drones;

(h) PDPA-Disposition 60/2016, concerning aspects of the international transfer of personal data. The transfer of personal data to countries that have not enacted adequate legislation on personal data protection is forbidden. Additionally, this Disposition approves two sets of standard model clauses for data controller to data controller transfers as well as data controller to data processor transfers;

(i) Access to Public Information Law No 27,275, creating the Agency of Access to Public Information ("AAPI") as its controlling authority. The Agency — which is autarchic and independent — is currently responsible for the application of the DPL and the Do-Not-Call Law; and

(j) AAPI-Resolution No 14/2018, setting out the information which owners and users of public and private databases have to include on their websites, as well as in any other communication or advertising, that guarantees the data subject's knowledge of his/her rights and how to exercise them.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The National Directorate of Data Protection ("DPND"), which is part of the National Department of Justice and Human Rights, was the data protection authority since it was formed in 2001. However, Emergency Decree No 746/2017 designated the AAPI as the authority charged with the application of the DPL and, since then, the AAPI has replaced the former enforcement authority, and is currently the government agency tasked with enforcing the DPL.

Among other responsibilities, the AAPI is in charge of:

(a) operating a registry of databases (keeping records of the registration and renewal 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 Agency is also responsible for assuring the effective exercise of the right of access to public information and the enforcement of transparency within the public sector.

The AAPI's inspections/audit proceedings can be ex officio or initiated upon a complaint. The administrative process that the AAPI must follow to investigate and impose penalties is set out in Sections 31 and 32 of the DPL, in Decree 1558/2001 and Decree 1160/2010. The administrative decisions can be appealed before the judicial courts.

In addition to the AAPI, 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 organisations (NGOs) 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 SCOPE

2.1 Which companies are subject to privacy law in Argentina?

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

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

2.2 Does privacy law in Argentina apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, companies outside the country that treat, or process, data of Argentinean residents must comply with local law and regulations.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" is defined in Section 2 of 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 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.

As stated in Section 7 of the DPL, 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.

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

Furthermore, Section 8 provides that 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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

As stated by Sections 4 and 10 of the DPL, 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 those purposes for which it was collected.

(d) Personal data must be stored in such a way as enables the data owner to exercise his/her 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.

(f) Those responsible or involved in any part of data processing are bound by the duty of confidentiality.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

According to Provision 4/2009 of the DPND, 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) stating the data subject's right to request the removal of, or a block on, the data subject's name from the database (Section 27 of the DPL).

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 DATA SECURITY AND BREACH

6.1 How is data security regulated in Argentina? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Issued in 2018, Resolution 47/2018 of the AAPI approved recommended security measures for the processing and conservation of personal data, which include recommendations in connection with personal data, whether or not stored by electronic means. These aim at ensuring the continuous improvement of the administration, planning and control of information security.

There are two sets of recommendations:

(a) Annex I deals with:
  (i) the collection of data;
  (ii) control of access to data;
  (iii) control of modifications;
  (iv) backup and recovery;
  (v) vulnerability management;
  (vi) information destruction;
  (vii) security incidents; and
  (viii) development environment;

(b) Annex II includes recommendations regarding:
  (i) the collection of data;
  (ii) control of access to data;
  (iii) information conservation;
  (iv) information destruction; and
  (v) security incidents.

It is important to point out that, whilst previous regulations provided for mandatory security measures, Resolution 47/2018 establishes a set of "recommendations" that can be adopted or not, or even replaced by other more effective measures based on the practices and circumstances of the processing of personal data. Moreover, the Resolution does not impose any particular data storage technological method or solution, allowing database controllers to make their own IT solution decisions.

6.2 How are data breaches regulated in Argentina? What are the requirements for responding to data breaches?

In Argentina, 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. Such an obligation has not been regulated and has not been established by any particular reports to the authorities or the affected individuals.

It is worth mentioning that there is a bill, submitted to Congress by the Argentine Executive Power in September 2018, which is intended to amend and replace the DPL, which addresses, in detail, data breach incidents and the proceedings to be followed if they happen, following the EU General Data Protection Regulation ("GDPR").

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The main rights for data owners contained in the DPL are the right of information, access and suppression. According to Section 14 of the DPL, data owners have the right to request and obtain information on any personal data included in a database. Moreover, the data controller must provide

this information within ten calendar days of notification, free of charge. Data subjects can exercise these rights every six months or more, unless a legitimate interest is proven.

Additionally, data owners have the right to request that their data is rectified, updated or deleted from databases. The data controller must rectify, update or delete the personal data within five days following a data owner's request.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

All marketing communications must comply with the regulations provided by Section 27 of the DPL, Decree No 1558/2001, Disposition No 4/2009 and Resolution No 14/2018, among others.

According to Disposition No 4/2009, all marketing communications in the country must include a notification to recipients of their right to request their exclusion from the relevant database, the way to exercise such right and the transcription of certain legal provisions (in Spanish). In addition, unsolicited or communications or those sent without consent must evidence their marketing nature in a noticeable manner; when sent through e-mail, their subject must include the term "Advertisement" ("Publicidad"). Companies carrying out direct marketing campaigns must inform recipients on their right to opt out, the procedure to exercise such right and quote certain legal provisions and ensure that they implement effective mechanisms to fulfill all potential opt-out requests.

In 2014, the Do-Not-Call Law created the Do-Not-Call Registry, expanding the protection of data owner's 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.

Resolution No 14/2018 establishes that the owners and users of public and private databases have to include in their websites, as well as in any other communication or advertising, particularly data collection forms, information that guarantees the data owner's knowledge of his/her rights and how to exercise them. Moreover, this Resolution requires controllers and users of public and private databases to clearly and expressly disclose the information required by Section 6 of DPL, including:

(a) the purpose of the data processing,

(b) any possible recipients of data,

(c) the existence of the database and the identity of the data controller,

(d) whether providing the data is mandatory or not, and

(e) rights data owners have,

prior to any data collection and specifically mentioning how data subjects may exercise their rights.

Likewise, the following wording must be included (in Spanish): "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 of the current data protection regulation".

These regulations are applicable in all cases of marketing addressed to Argentine residents, irrespective of the country or jurisdiction from which the marketing communications are delivered.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertising and behavioral advertising are not specifically regulated by local law. The regulations described in question 8.1 also apply to these type of advertising activities.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The processing of personal data for advertising or marketing purposes, including data sharing, is allowed without prior consent when the data is limited to the creation of consumer profiles that categorise personal preferences and similar types of behavior, and/or when the data owners are solely identified by their belonging to generic groups and the individual data is strictly necessary to market or advertise to the individual (Section 27, DPL Regulatory Decree 1558/2001).

8.5 Are there specific privacy rules governing data brokers?

No.

8.6 How is social media regulated from a privacy perspective?

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

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Pursuant to the DPL, the transfer of personal data to countries that have not enacted adequate legislation on personal data protection is forbidden. Disposition 60/2016 provides that personal data can be transferred to the following countries without any further safeguard being necessary: member states of the European Union and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faroe Islands, Canada (only private sector), New Zealand, Andorra and Uruguay. Local

authority has considered the EU Commission's decisions on the adequacy of the protection of personal data in third countries to determine which jurisdictions are deemed adequate for the data transfer.

The Disposition has also 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.

Furthermore, Resolution 159/2018 issued by the AAPI set 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 AAPI 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 AAPI for its approval.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

As mentioned in question 9.1, Disposition 159/18 sets out guidelines for companies to draft and implement binding corporate rules or "BCR"s, which regulate intra-group international transfers of personal data.

Local law and regulations encourage companies to implement a privacy policy which regulates their personal data collection, treatment and processing and security mechanisms. The AAPI can request company's privacy policy and BCRs upon inspections.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Penalties are established in Sections 31 and 32 of the DPL, in Decree 1558/2001 and Decree 1160/2010. The AAPI may apply sanctions for any violations of the Argentine Data Protection Regulations. The sanctions can include, warnings, suspensions, fines and closure or cancellation of the file, register or database, without prejudice to any applicable civil or criminal liabilities. There are precedents for the authority fining companies which fail to comply with the data protection legislation, although such fines are usually low.

In addition, Section 157 of the Criminal Code provides that imprisonment of between one month and two years may be imposed on any person who:

(a) knowingly and unlawfully, or by violating data confidentiality and security systems, accesses a personal database;

(b) unlawfully provides or discloses to third parties information registered in a personal database that should be kept confidential by provision of law; or

(c) unlawfully inserts data in a database.

Penalties imposed by Sections 117 and 157 of the Criminal Code will be increased if the perpetrator is a public officer.

10.2 Do individuals have a private right of action? What are the potential remedies?

Anyone with a legitimate interest — individual or company — may file an administrative claim before the AAPI. The AAPI 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Argentina which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

In 2018, the Argentine Executive Office introduced a new bill intended to replace the DPL enacted in 2000, which has become outdated in relation to technological and legal developments, especially regarding the passing of the GDPR.

The Bill introduces new definitions aligned with the EU regulations, such as the concept of database, personal data and sensitive data. At the same time, the Bill introduces new concepts regarding genetic data, biometric data, economic groups, security incidents and international transfer. Also, it limits the scope of the concept of data subjects to human persons.

Among other changes, the Bill introduces new grounds for the collection and processing of personal data other than consent, such as legitimate interests; the obligation to report any security incident to the controlling authority and to data subjects; and increases the penalties for infringements.

If passed into law, the Bill provides for a two-year transition period.

Another bill already in Congress — likely soon to be enacted, and related to data protection — is intended to regulate internet service providers' liability.

Finally, several regulations are expected to be issued under the Information Technologies and Communications Law No 27,078, which are likely to have a direct impact on data processing for telecommunication providers.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Argentina?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/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 increasing demanding data privacy to avoid personal data violation. The global scenery drives Argentina to the imminent enactment of a new law, in line with the GDPR.

12.2 What do you envision the privacy landscape will look like in 5 years?

Recent administrative changes in the AAPI, together with expected legislative changes, along with the DPL Bill, which is aligned with GDPR, 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.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

In the current changing privacy landscape, companies' challenges will be aligned with the ones they are now facing in the European Union.

AUSTRALIA

1 PRIVACY LAW

1.1 How is privacy regulated in Australia?

Privacy is regulated in Australia through legislation at a 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 organizations with a turnover of AU$3 million or more, as well as certain other private organizations regardless of turnover. Small businesses (with a turnover of less than AU$3 million) are not regulated by the Privacy Act. The Privacy Act includes 13 Australian Privacy Principles ("APP"s) which set out the standards, rights and obligations around the collection, use, storage and disclosure of personal information.

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

Each Australian State and Territory has its own legislative or administrative regime which is discussed in further detail below.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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

(a) Federal level:

(i) The Privacy Act is the primary piece of legislation that regulates privacy at the Federal level. The Privacy Act also regulates how private sector health service providers collect and handle health information, but does not apply to State and Territory public sector health service providers.

(ii) The Income Tax Assessment Act 1936 (Cth) and Taxation Administration Act 1953 (Cth) regulate the handling of Tax File Numbers, including offences for unauthorised use, disclosure, collection or requests for Tax File Numbers.

(b) Each Australian State and Territory has its own legislative system or administrative regime to manage the privacy of individuals:

(i) New South Wales

- The Health Records Information Privacy Act 2002 regulates private sector health organizations, health service providers and businesses with a turnover of more than AU$3 million that hold health information.
- The NSW Privacy and Personal Information Protection Act 1998 regulates how State agencies manage personal information in accordance with the 12 information protection principles.
- The NSW Information Privacy Commissioner administers both complaints made under the Health Records Information Privacy Act 2002 and the Privacy and Personal Information Protection Act 1998.

(ii) Victoria

- The Health Records Act 2001 regulates organizations that hold health information.
- The Victorian Charter of Human Rights also contains a right to be free from unlawful or arbitrary interference with privacy.
- The Victorian Privacy and Data Protection Act 2014 establishes 10 information privacy principles that regulate how public sector organizations and private organizations carrying out functions for and on behalf of Victorian public sector organizations can handle personal information and creates a complaint scheme.

(iii) Australian Capital Territory

- The Health Records (Privacy and Access) Act 1997 regulates organizations that hold health information and manages complaints for health record privacy issues. The ACT Office of the Health Services Commissioner conciliates complaints.
- The ACT also protects personal information through the Information Privacy Act 2014. This regulates how private sector agencies handle personal information, as well as private companies contracted to provide services for the ACT government. This is administered by the ACT Information Privacy Commissioner.

(iv) Tasmania

- The Personal Information Protection Act 2004 contains 10 information protection principles, and provides the right for an individual to complain to the Tasmanian Ombudsman if personal information has been mismanaged. The information protection principles apply to State bodies and private organization where they have entered into contract with a personal information custodian relating to the collection, use or storage of the personal information.

(v) Western Australia

- The Freedom of Information Act 1992 includes some principles related to the disclosure and amendment of personal information disclosed to State and local government agencies.

(vi) Northern Territory

- The Information Act 2002 regulates how health information is managed; complaints are heard by the NT Office of the Information Commissioner.

(vii) South Australia

- The State government has a set of information privacy principles. Complaints are managed by the South Australian Privacy Committee.

(viii) Queensland

- The Information Privacy Act 2009 regulates how the public sector manages personal information. The Queensland Office of the Information Commissioner receives complaints.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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 Commissioner may also take more serious regulatory action such as (but not limited to) accepting an enforceable undertaking, making a determination, or 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 (see question 1.2).

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

2 SCOPE

2.1 Which companies are subject to privacy law in Australia?

The Privacy Act applies to "entities" which consist of Australian Federal government agencies, organizations with an annual turnover of more than AU$3 million and their related companies, as well as some other organizations regardless of turnover, including health service providers and organizations that trade in personal information.

An "organization" includes an individual (including a sole trader), a body corporate, a partnership, unincorporated association or a trust.

It does not include a small business operator, registered political party, or a State or Territory authority.

2.2 Does privacy law in Australia apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, the Privacy Act 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.

Put another way, if an individual is located in Australia, the collection of their personal information by a foreign entity is deemed to have happened in Australia.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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".

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

There are 13 Australian Privacy Principles ("APP"s) contained within the Privacy Act that companies (which are subject to the Privacy Act) need to follow regarding their processing of personal information:

(a) **APP 1 — Open and transparent management of personal information**: This includes having a clear and up to date company privacy policy.

(b) **APP 2 — Anonymity and pseudonymity**: Companies should allow individuals the option to remain anonymous or to use a pseudonym, except where impracticable or a prescribed exception applies.

(c) **APP 3 — Collection of solicited personal information**: Companies may only solicit and collect personal information where it is reasonably necessary for the companies' functions or activities. In addition, companies 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.

(d) **APP 4 — Dealing with unsolicited personal information**: If a company receives unsolicited personal information, the company is required to determine whether it would otherwise have grounds on which to collect it. If the company does have such grounds, it may retain the personal information, provided it complies with the remaining APPs. If the company does not have such grounds, it must destroy or de-identify the personal information.

(e) **APP 5 — Notification of the collection of personal information**: A company that collects personal information about an individual is required to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters (including the company's identity and contact details, the fact and circumstances of collection, the purposes of collection, and whether the company is likely to disclose personal information to overseas recipients).

(f) **APP 6 — Use or disclosure of personal information**: A company can only use or disclose personal information for a purpose for which it was collected (ie, the primary purpose), unless the individual has consented to a secondary use or disclosure, or the individual would reasonably expect their personal information to be used for the secondary purpose, or 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 authorised by or under an Australian law or a court/tribunal order).

(g) **APP 7 — Direct marketing**: A company 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.

(h) **APP 8 — Cross–border disclosure of personal information**: A company that discloses personal information to an overseas recipient must take reasonable steps to ensure that the overseas recipient does not breach the APPs. The company will be accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.

(i) **APP 9 — Adoption, use or disclosure of government related identifiers**: Companies 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).

(j) **APP 10 — Quality of personal information**: Companies 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**: Companies must take reasonable steps to protect the personal information they hold from misuse, interference, loss, unauthorised access, modification or disclosure.

(l) **APP 12 — Access to personal information**: Companies that hold personal information about an individual are required to give the individual access to that information on request, unless an exception applies.

(m) **APP 13 — Correction of personal information**: Companies 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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

As a general rule, the APPs provide that an organization should only use or disclose personal data for the purpose for which it was collected. However, an organization may use or disclose personal data about an individual for another purpose ("secondary purpose") if the individual has consented, or the secondary purpose is related to the primary purpose and such use or disclosure might reasonably be expected by the individual. If the personal data is sensitive personal data, the secondary purpose must be directly related to the primary purpose. There are also a number of exceptions to this general rule. In terms of advertising, APP 7 provides a general prohibition against direct marketing unless an exception applies. Individuals must always be given a simple means to opt-out of any direct marketing.

APP 1 requires that entities regulated under the Privacy Act have an up-to-date and clearly expressed privacy policy that is easily accessible. A privacy policy should, among other things, set out what information is collected about individuals, the purpose for the collection of information and whether personal information is disclosed to third parties.

There is no obligation to appoint a privacy officer in an organization, however the OAIC recommends the appointment of a privacy officer as part of its best practice guidelines, in order to ensure there is a simple point of contact for privacy related complaints/enquiries, and someone who is responsible in the organization for compliance with privacy laws. The Privacy Act does not set out the scope within which a privacy officer must act, but the OAIC has developed guidelines for recommended practices and systems, available at: https://www.oaic.gov.au/s/privacy-officer-toolkit/.

A privacy impact assessment is a voluntary process undertaken to evaluate a company's compliance with the APPs. The OAIC suggests privacy impact assessments should be conducted as part of the planning process to identify and mitigate privacy risks, particularly where a project or activity may impact on the privacy of individuals. The OAIC provides guidance on how to conduct a privacy impact

assessment, available at: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.

Although not mandatory, the OAIC also recommends conducting a risk analysis as best practice for preparing a data breach response plan.

There is no requirement in Australia for organizations to register anything with a privacy authority such as the OAIC.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Australia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Under APP 11, entities must take reasonable steps to ensure the security of the personal information they hold. The concept of taking reasonable steps is relative to the size of the business and the sensitivity of the information held. Reasonable steps could include internal training, ICT 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 at: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/.

6.2 How are data breaches regulated in Australia? What are the requirements for responding to data breaches?

Part IIIC of the Privacy Act contains the Notifiable Data Breaches scheme, which requires certain entities covered by the Privacy Act to notify affected individuals and the OAIC about data breaches and when loss of information or unauthorised access to information is likely to result in serious harm to an individual whose personal information is involved.

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 the data breach would likely result in serious harm to an individual whose information was involved in the breach.

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, 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) If serious harm is likely, 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 publicise it.

(e) If the breach is not likely to result in serious harm, or after notifying the OAIC and affected individuals, the entity should conduct a review of the incident and take action to prevent future breaches.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

(a) Individuals have the right to access their personal information from an organization or agency holding their personal information under APP 12.

The organization or agency must give an individual access to their personal information when it has been requested by the individual, except where the law allows the organization or agency to refuse the request. Examples of instances where access can be refused are provided in APP 12, and include:

(i) the organization believes that giving the individual access may endanger the life, health or safety of any individual, or endanger 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; or

(iv) the personal information is part of existing or anticipated legal proceedings between the individual and the organization.

(b) Under APP 13, individuals can also request a correction of their personal information an organization or agency holds about them if the personal information is:

(i) inaccurate;

(ii) out of date;

(iii) incomplete;

(iv) irrelevant; or

(v) misleading.

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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications via electronic commercial communications (including email and SMS) are regulated by the Spam Act (2003) ("Spam Act"). The Spam Act regulates how marketing messages are transmitted by anyone in, into or from Australia. Generally, the person who will receive the message must consent to receiving the message, the message must identify and provide the contact details of the sender, and the message must include a functional unsubscribe facility.

The Do Not Call Register Act (2006) ("Do Not Call 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Use of tracking technologies 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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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.

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 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 is Australia's first self-regulatory guideline for third party online behavioral advertising. The guideline sets out self-regulatory principles for online behavioral advertising, and aims to promote transparency and consumer awareness and to encourage best practice and accountability.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

If the advertiser is providing de-identified information to the third party, which is matched with relevant customer profiles, there is no use of personal information and the Privacy Act does not apply.

However, if personal information is being used to identify individuals to advertise to, the APPs will apply:

(a) Under APP 5, a company is required to take reasonable steps to notify an individual if they are collecting personal information about the individual. The company must notify an individual of certain matters, including:

(i) the company's identity and contact details;

(ii) the fact and circumstances of collection;

(iii) whether the collection is required or authorised 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) information about the company's Privacy Policy; and

(viii) whether the company is likely to disclose personal information to overseas recipients, 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.

(b) Under APP 6, if data sharing and disclosure to third parties is the primary purpose of the collection of data, and the individual is made aware of this and has consented to it, the company can disclose the personal information to third parties. However, if data sharing is a secondary use, the company will need to obtain additional consent from the individual to that secondary use of the personal information, unless an exception applies.

Consent can be express or implied. The four key elements of consent are:

(i) the individual is adequately informed before giving consent;

(ii) the individual gives consent voluntarily;

(iii) the consent is current and specific; and

(iv) the individual has the capacity to understand and communicate their consent.

8.5 Are there specific privacy rules governing data brokers?

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).

8.6 How is social media regulated from a privacy perspective?

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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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 will apply.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Personal information can be transferred between group companies without such transfer becoming a "disclosure". Other than this, personal information should only be transferred to third parties with the consent of the individual, or where the transfer is reasonably contemplated or is part of the primary purpose of the collection. Once personal information is transferred to a third party it is considered a "disclosure" and the entity must comply with all the elements of APP 6.

The disclosure of personal information to other jurisdictions outside Australia is governed by APP 8, which requires that entities take reasonable steps to ensure that a foreign recipient of personal data complies with the APPs. APP 8.2 provides that this is not necessary where:

(a) it is reasonably believed that the recipient is subject to a law or binding scheme that bears overall substantial similarity to the APPs and the individual can take action to enforce such protections;

(b) the entity has obtained the individual's consent to the foreign disclosure;

(c) the foreign disclosure is required or authorised by Australian law;

(d) such disclosure is required by a government agency under an agreement to which Australia is a party;

(e) the disclosure is by a government agency and relates to foreign law-enforcement activities; or

(f) a permitted general situation applies (such as to prevent serious health and safety risks).

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

A transfer of personal information (other than sensitive information) from a company to a related body corporate is not taken to be an interference with the privacy of an individual. The Privacy Act requires that the personal information that is disclosed to a related body corporate must be handled in accordance with the primary purpose for which it was initially collected by the company that collected the personal information.

However, where the company discloses personal information to a related body corporate located outside Australia, APP 8 will apply, which puts an obligation on the company to take reasonable steps to ensure the overseas related body corporate does not breach the APPs in relation to the personal information.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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.

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 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 determination or bring proceedings to enforce a determination;

(c) seek an injunction to prevent a potential privacy breach from continuing; or

(d) apply to the court for a civil penalty.

For serious and repeated breaches of privacy by an entity, the Commissioner may apply to the Federal Court or Federal Circuit Court for an order that the entity pay the Commonwealth a penalty. For a "serious or repeated interference with privacy" a person must pay up to 2,000 penalty units (which currently amounts to approximately AU$420,000).

10.2 Do individuals have a private right of action? What are the potential remedies?

(a) **Common law rights**: There is currently no common law right of privacy in Australia; however, recent case law suggests a common law tort for invasion of privacy may be developing. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 the most superior court in Australia, being the High Court, left the possibility of a tort of privacy open. To date no Australian appellate court has confirmed the existence of a tort of privacy.

However, lower courts have awarded damages for tortious invasions of privacy, suggesting that the legal basis for this action does exist. For example, the County Court of Victoria awarded damages for breach of personal privacy in *Jane Doe v ABC* (2007) VCC 281.

The Queensland District Court has also awarded damages on the basis of invasion of privacy in *Grosse v Purvis* (2003) QDC 151.

The Australian Law Reform Commission ("ALRC") and the Australian Competition and Consumer Commission ("ACCC") have both called for the statutory creation of a right of privacy. The ACCC recommendation was released in July 2019.

(b) **Statutory rights**: Whilst there is currently no statutory regime in Australia for an individual to enforce a private right of action for breach of privacy, an individual can make a complaint to a company regarding a potential breach of privacy, and lodge the complaint with the OAIC. The OAIC will then investigate the matter and take action on behalf of the individual.

While a civil penalty order does not compensate individuals, Sections 25 and 25A of the Privacy Act allow an individual to recover compensation for loss or damage (including injury to the individual's feelings or humiliation) suffered by the individual, or other remedies where a civil penalty order is made against a company for a contravention of a civil penalty provision. Other remedies include a court order directing the company to:

(i) carry out any reasonable course of conduct to redress the loss or damage suffered by the individual;

(ii) pay the individual a specified amount to reimburse the individual for expenses reasonably incurred by the individual in connection with the contravention or commission of the offence; and

(iii) pay to the individual the amount of loss or damage suffered by the individual.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Australia which affect privacy?

There is currently no privacy-related legislation in Australia which is specific to Australian culture. However, the ALRC published recommendations in a 2010 report, which discussed establishing a privacy protocol to protect the privacy of indigenous groups. Recommendation 7-1 recommended that the Office of the Privacy Commissioner (now the OAIC) should encourage and assist agencies and organizations to develop and publish protocols, in consultation with indigenous groups and representatives, to address the particular privacy needs of indigenous groups. Recommendation 7–2 recommended that the Australian government should undertake an inquiry to consider whether legal recognition and protection of indigenous cultural rights is required and, if so, the form such recognition and protection should take.

Currently 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 Are there any hot topics or laws on the horizon that companies need to know?

In July 2019, the ACCC released the Digital Platforms Inquiry Report, which contains a number of recommendations. The report is most relevant to online businesses, search engines, content aggregation platforms and social media platforms. A strong theme in the report is the need to increase the transparency of organizations that are entrusted with personal information, in order to allow consumers to make informed choices about their personal information. In particular, the report made a number of relevant recommendations, including:

(a) the development of a Privacy Code for Digital Platforms, including specific periods for data retention and more prescriptive obligations regarding form of privacy policies;

(b) increased penalties for breaches of privacy to mirror the penalties for breaches of the Australian Consumer Law (the greater of AU $10 million, three times the benefit received, or 10% of annual turnover in the preceding 12 months);

(c) technical and location data being included in the definition of personal information;

(d) stronger consent requirements for any data collection, rather than only secondary data collection;

(e) measures to require organizations to erase personal information on request; and

(f) creation of a statutory tort for serious invasion of privacy, not confined to organizations subject to the Privacy Act.

If implemented, these recommendations will pose a significant compliance challenge to businesses that collect personal information.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Australia?

If collecting sensitive information, there are greater obligations to ensure that individuals are aware that their personal information is being collected, the purposes for which the information is collected, and 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.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The rapid development in online technology has had a major impact on personal privacy. In particular, the large amount of personal information being collected, store and shared/traded between companies in an online environment has made it easier for large data breaches to occur. According to the Australian Bureau of Statics, one in ten Australian businesses suffered some form of data breach in 2018.

The Notifiable Data Breaches scheme came into effect in February 2008, which has the primary objective of increasing consumer protection. It introduced a much-needed legal obligation on entities to carry out an assessment whenever they suspect a data breach, and to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The scheme effectively ensures that entities have reasonable steps in place to secure personal information, which in turn improves security standards.

As a result of the ACCC's Digital Platforms Inquiry Report released this year (see question 11.2), the Australian government announced its intention to make major changes to privacy laws which will implement stronger privacy protections for individuals. One of the proposed changes is the introduction of increased penalties for serious or repeated breaches of privacy.

Another proposed change is to give the OAIC more powers to issue infringement notices for failure to cooperate with efforts to resolve minor breaches. The maximum fines that could be issued under an infringement notice are AU $63,000 for companies and AU $12,600 for individuals. Specific rules will also be introduced to protect the personal information of children and other vulnerable groups.

The changes to Australian privacy laws are to ensure that the law is relevant and effective in the digital environment, and to bring Australia more in line with the EU GDPR regime.

12.2 What do you envision the privacy landscape will look like in 5 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. Currently the issue of "Big Data" remains a grey area; however, it is clear that, as companies gather more information about a person and "consumer profiling" occurs with multiple overlays of information, the data that was originally not considered personal information, such as location or IP address, will potentially fall into the definition of "personal information" as the data subject becomes more easily identifiable through the narrowing down of possibilities. Therefore, there are questions about how to regulate this space, and we anticipate the definition of personal information will need to change in order to protect information about a person who has become an identified individual through the collection of large amounts of de-identified data.

We also anticipate changes will be made to strengthen notification and consent requirements relating to personal information, and further discussions on a direct right for individuals to bring actions for a breach of their privacy.

12.3 What are some of the 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. More changes to the law mean that companies will need to work harder to ensure compliance with the privacy laws. With harsher penalties coming into place, companies are being forced to re-evaluate their privacy policies and processes.

In the wake of serious data breaches, companies are also having to consider new software and technology to increase their data security and protect the personal information of individuals which they hold, resulting in additional compliance costs.

BELIZE

1 PRIVACY LAW

1.1 How is privacy regulated in Belize?

Belize is lacking thorough regulation of privacy. Currently, privacy is only expressly considered in the Belize Constitution, though references can be found in some laws which regulate public and private entities, and which are required to obtain personal information.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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

(a) The Belize Constitution Act, Cap. 4, 2012;

(b) Interception of Communications Act, Cap. 229.01;

(c) Freedom of Information Act, Cap 13;

(d) Caribbean Community Act, Cap. 17;

(e) Justice Protection Act, Cap. 119.02;

(f) The Census Act, Cap. 155;

(g) Statistical Institute of Belize Act, Cap. 158;

(h) Belize Telecommunications Act, Cap. 229;

(i) Copyright Act, Cap. 252;

(j) Immigration Act, Cap. 156;

(k) Immigration (Advance Passenger Information) Regulations 2017 (SI No 46-2017); and

(l) tax information exchange agreements (that have been signed with various countries).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

There are no regulatory bodies set up specifically to enforce privacy law. Its enforcement falls under the jurisdiction of the Belizean Judicial System and the regulating bodies of the industries which utilize personal information in fulfilment of 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 SCOPE

2.1 Which companies are subject to privacy law in Belize?

To the extent that privacy laws exist in Belize, they apply to both the public and private sectors.

2.2 Does privacy law in Belize apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

N/A

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Belize?

The term is not specifically defined in any legislation.

However, Section 2 of the Statistical Institute of Belize Act defines "confidential data" as "data obtained by the Institute for the production of official statistics when such data allow statistical units to be identified directly or indirectly, thereby disclosing individual information"; and it can be inferred from Section 42(1) that "personal information" is information which can be related to an identifiable person.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Though not expressly categorized in any law, any information that is a personal identifier is considered sensitive, and subject to confidentiality and disclosure only on the authorization of the person to whom it refers, or under court order that abides by Section 14 of the Constitution.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Due to the implementation of the EU General Data Protection Regulation ("GDPR"), most companies, especially in the tourism industry and banking industry, that are exposed to handling information of EU citizens are implementing this regulation. Therefore, most companies implement the principles set forth in the GDPR, namely: lawfulness, fairness and transparency, purpose limitation, accuracy, data minimisation, integrity and confidentiality and storage limitation.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

There are no national regulations; however, most sectors tend to pull resources for their businesses (such as website terms and conditions; system and platform provisions) from the United States and the European Union (English-speaking) nations. Therefore, many companies (by default) comply with international regulations, such as the GDPR and other data protection and privacy laws.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Belize? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is not specifically regulated. Part III of the Interception of Communications Act, which especially applies in cases of wire-tapping and other means of data gathering to investigate criminal offences, stipulates the sanctions for having acquired protected information or traffic data by means of a communication network for personal use, commercial benefit, political advantage, or criminal activity. This provision is the most specific one found in this regard amongst the cadre of Belizean laws.

6.2 How are data breaches regulated in Belize? What are the requirements for responding to data breaches?

Data breaches are regulated in the Interception of Communications Act (see question 6.1). They are referred to as "unauthorized interceptions".

However, there is a draft Cyber Security Bill currently undergoing stakeholder review, which is intended to be enacted in 2020. This Act will be one of the first to delve deeply into data security and privacy in the digital environment.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

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.

In this regard, the Belize Constitution Act regulates the following in Section 3:

> "Whereas every person in Belize is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely,
>
> (a) life, liberty, security of the person, and the protection of the law;
>
> (b) freedom of conscience, of expression and of assembly and association;
>
> (c) protection for his family life, his personal privacy, the privacy of his home and other property and recognition of his human dignity; and
>
> (d) protection from arbitrary deprivation of property,
>
> the provisions of this Part shall have effect for the purpose of affording protection to those rights and freedoms subject to such limitations of that protection as are contained in those provisions, being limitations designed to ensure that the enjoyment of the said rights and freedoms by any person does not prejudice the rights and freedoms of others or the public interest."

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

There is no national regulation, however there are a myriad of businesses that comply with the GDPR and/or other international regulations.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is no national regulation.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There is no national regulation.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

N/A

8.5 Are there specific privacy rules governing data brokers?

N/A

8.6 How is social media regulated from a privacy perspective?

There are no national regulations. However, the Belizean community is very vocal about any injustice carried out through social media, especially with respect to cyber-bullying, discrimination and the exposure of personal information. Public outcry has led to a strong push towards the passing of the Cybersecurity Bill, especially after social media has been used to expose intimate pictures of individuals, as well as to direct threats towards individuals' personal and sexual integrity, especially of women. The last instance of cyber-bullying was met with outcry from both the public and private sectors, including the Prime Minister, Minister of Government and several NGOs.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

N/A

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

No. Any requirements or restrictions exist within the agreements/contracts between parties.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The potential penalties are fines and prison sentences. For example, in accordance with the Interception of Communications Act, fines of up to 200,000 dollars may be imposed, and imprisonment for up to ten years, depending on the matter and its recurrence.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes, individuals have a private right of action under Constitutional Law, Torts and Contract Law. The potential remedies are damages.

Due to the lack of specific legislation on privacy, many people rely on privilege established between a professional and themselves. In addition, where sensitive information is exchanged, it is the norm to include a confidentiality clause in the contract, or to carry out a confidentiality agreement.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Belize which affect privacy?

No. Privacy and its preservation in daily life and in commerce is not a prevalent, nor thoroughly explored part of Belizean society. Therefore, even from a cultural perspective, there appears to be no specific "rule" that affects privacy in Belize.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

There is currently a Cybercrime Bill that is expected to be passed into law in 2020. This bill regulates the illegal access to computer systems, interception, data interference, acquisition of data, computer-related forgery and fraud, and identity related offenses, among others.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Belize?

Belize caters to a large number of 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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

In 2019, there were occurrences relating to: cyber-bullying; social media and website hacking; bank account data phishing; and ATM tampering and fraud. Due to these events, matters of privacy came into sharper focus in public discussion, however, there has not been an equally intense focus on passing legislation to deal with these issues.

12.2 What do you envision the privacy landscape will look like in 5 years?

Due to Belize's lack of attention to the need for privacy regulation, we anticipate that there will continue to be sensational events concerning breaches of privacy and data breaches, which will touch several area of society including:

(a) youth and cyber-bullying;

(b) banks and data protection; and

(c) telecommunications and data transfer.

Therefore, it is highly likely that, within the next 5 years, Belize may, in "one fell swoop", revamp its privacy landscape in order to combat the various issues; and will possibly do so in a wide-reaching and cohesive manner.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Companies must carry out their due diligence to ensure that they abide by the upcoming legislation to avoid corporate liability, especially if and when the Cybersecurity Bill is passed, as it stipulates that the courts in Belize will have jurisdiction, among other situations, if a regulated act is carried out and 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.

BOLIVIA

1 PRIVACY LAW

1.1 How is privacy regulated in Bolivia?

Privacy is regulated as a fundamental right, recognized in Article 21.2 of the Bolivian Constitution. As a consequence, constitutional rulings issued by the Bolivian Constitutional Court have developed the scope of this right and create certain specific obligations aimed at the adequate protection of privacy.

Additionally, sector-specific laws for certain regulated sectors (such as financial entities and telecommunications) impose more obligations upon those entities subject to such legislation.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) National laws:

(i) Bolivian Constitution (Articles 21.2, 130 and 131);

(ii) Criminal Code (Articles 363 Bis and 363 Ter);

(b) Sector-Specific Laws

(i) Access to Information, Supreme Decree 28168 (Article 19) (executive branch and State-owned companies);

(ii) Electoral Organization Law 018 (Articles 72, 74, 76, 77 and 79) (electoral body);

(iii) Telecommunications Law 164 (Articles 54, 56, 59, 84, 89, 90, and 91) (telecommunications industry);

(iv) Telecommunications Regulation Supreme Decree 1391 (Article 179) (telecommunications industry); and

(v) Telecommunications Regulation Supreme Decree 1793 (Articles 3, 4, 40, 54, 56 and 57) (telecommunications industry).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Privacy law is enforced through:

(a) Constitutional rulings issued by the Bolivian Constitutional Court, when it is considered that a certain person, company or entity is affecting privacy as a fundamental right of another person.

(b) Criminal judgements, when the particular situation is considered to be a criminal offense.

(c) Administrative resolutions issued by the Telecommunications and Transport Authority (only applicable to the companies that are under its authority).

2 SCOPE

2.1 Which companies are subject to privacy law in Bolivia?

All companies are subject to the privacy guidelines (among others) resulting from constitutional rulings. This means that the standards and rules that the Bolivian Constitutional Court has developed through its rulings are mandatory for all companies and people in the Bolivian territory.

However, some companies are also subject to specific privacy laws. For example, Law 164, Supreme Decree 1793 and Supreme Decree 1391 establish privacy protection obligations for companies that perform activities or supply services related to telecommunications, information technologies, and communication. There are also several regulations issued by the Bolivian Financial Regulatory Agency that impose specific privacy protection obligations on financial institutions, including insurance providers and related entities.

Finally, there are laws are only applicable to certain state entities in the executive branch (Law 018) and the electoral body (Law 28168).

2.2 Does privacy law in Bolivia apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Bolivian privacy laws are applicable to foreign entities only to the extent that the activities of such foreign companies are performed in Bolivia or that Bolivian persons are the intended consumers of the products or services.

Law 164 and Supreme Decree 1391 apply to companies that carry out activities or supply services related to telecommunications, information technologies and communication. These regulations apply to companies whose activities: (i) originate in Bolivia, (ii) transit through Bolivia or (iii) have consumers in Bolivia.

There are no specific regulations resulting strictly from privacy law for companies outside the country.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Bolivia?

Article 3 of Supreme Decree 1793 defines "personal data" as all information that identifies, or makes identifiable, a person or legal entity.

The Bolivian Constitutional Court has not defined the term "personal data", although there are specific rulings that use this concept and link it to the right of privacy.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Constitutional Sentence 1738/2010-R defines "sensitive information" as information that only concerns its owner, such as political and religious beliefs, sexual orientation, health conditions, information that could generate any type of discrimination, etc.

The owner of this information has the right to request the exclusion of this information, and there is an obligation on an entity that has such information not to share it, or make it public.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Local legislation does not establish specific principles regarding the processing of personal data. However, it is understood that consent is key. The owner of the information must be aware of every aspect related to the processing of his/her information in order to provide informed consent.

However, we recognize as good practice the implementation of the principles established by the Inter-American Juridical Committee regarding privacy and data protection. This document includes the following principles (among others):

(a) Lawful and fair purposes ("Personal data should be collected only for lawful purposes and by fair and lawful means");

(b) Clarity and consent ("The purposes for which personal data is collected should be specified at the time the data is collected. As a general rule, personal data should only be collected with the consent of the individual concerned");

(c) Relevant and necessary ("The data should be accurate, relevant and necessary to the stated purposes for which it is collected");

(d) Limited use and retention ("Personal data should be kept and used only in a lawful manner not incompatible with the purpose(s) for which it was collected. It should not be kept for longer than necessary for that purpose or purposes and in accordance with relevant domestic law");

(e) Duty of confidentiality ("Personal data should not be disclosed, made available or used for purposes other than those for which it was collected except with the knowledge or consent of the concerned individual or under the authority of law");

(f) Protection and security ("Personal data should be protected by reasonable and appropriate security safeguards against unauthorized access, loss, destruction, use, modification or disclosure"); and

(g) Accuracy of data ("Personal data should be kept accurate and up-to-date to the extent necessary for the purposes of use").

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No, Bolivian legislation does not assign different roles to companies in this way.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The main obligation required by privacy law is related to consent; according to Bolivian legislation, consent of the owner of the personal data is required at all stages of data processing and storage.

Therefore, the main obligation for companies is to obtain this consent (in writing, when sector-specific legislation requires it).

Another obligation is to store and process this information through secure mechanisms, in order to avoid it being used in any way in which consent has not been obtained.

Companies are required to inform information-owners of their rights, especially their right to access, rectify, cancel or delete this information.

These are general obligations, there are no specific privacy obligations in advertising.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Bolivia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is regulated in Bolivia as an obligation on those subject to Supreme Decree 1793, namely companies or individuals that carry out activities or provide services related to digital certification, eGovernment, free software, email and use of documents and digital signatures. According to this Supreme Decree, the person responsible for data processing must implement all measures that guarantee the security of personal data. The measures taken must be appropriate given technological advances and the nature of the data stored.

There is nothing in local legislation to help companies address this standard.

6.2 How are data breaches regulated in Bolivia? What are the requirements for responding to data breaches?

Depending on the circumstances, data breaches can be treated as:

(a) Criminal offense under the Criminal Code: namely either:

  (i) Access and misuse of computer data: One who, with the intention to obtain an undue benefit for himself/herself or a third party, manipulates a processing or transfer of computer data that leads to an incorrect result or avoid such a process whose result would have been correct, causing a transfer of assets to the detriment of a third party, may be punished with one to five years of imprisonment and a fine of 60–200 days).

  (ii) Data manipulation: One who, without being authorized, seizes, accesses, uses, modifies, delete or disables data stored on a computer or in any computer support, causing damage to the owner of the information, may be sanctioned with community service of up to one year or a fine of up to 200 days).

(b) Violation of the constitutional right to privacy: This may be protected through a constitutional claim. This is considered subsidiary; other possibilities in order to solve a particular claim must prevail and used before presenting a constitutional claim.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals in Bolivia have the following rights related to their personal information/personal data:

(a) to access their collected and stored information, including the right to know the specific aims and objectives of the data collection and storage;

(b) to object to the collection and storage of their information;

(c) to request and obtain the cancelation and deletion of their personal information;

(d) to rectify inaccurate or incomplete personal information; and

(e) to request confidentiality of the collected information.

According to the Bolivian Constitutional Court, all these rights are included in a generic right known as the "Informative Auto-Determination".

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications are not regulated in Bolivia from a privacy perspective. However, it is understood that general rules regarding data protection developed by the Constitution and Bolivian Constitutional Court are applicable to marketing communications.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Tracking technologies are not regulated in Bolivia.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertising and behavioral advertising are not regulated in Bolivia.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

In order for advertisers to share data with third parties for customer matching, the owner of the personal data must provide unequivocal consent. In cases where the company is subject to Supreme Decree 1793 (see question 6.1), this consent must be in writing. This obligation is applicable to any type of data transfer or sharing; customer matching is not specifically contemplated in Bolivian legislation.

8.5 Are there specific privacy rules governing data brokers?

There are no specific privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

There is no regulation related to social media from a privacy perspective in Bolivia. The relationship between Bolivian users and social media platforms is strictly regulated by the terms and conditions of each platform, and there is no additional regulation established by Bolivian legislation.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs and promotions are not specifically regulated from a privacy perspective. However, it is understood that general rules regarding data protection developed by the Constitution and Bolivian Constitutional Court are applicable to loyalty programs and promotions.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

By Article 56 of Supreme Decree 1793, the owner of personal data must be informed, before giving his/her consent, about (among other things) the potential recipients of the information, and the identity, address and legal representative of the entity responsible for the data treatment.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

By Supreme Decree 1793, the consent given by the owner of the personal data must be clear and provided in writing or any appropriate medium. Even though this Supreme Decree does not apply to all companies in Bolivia (see question 6.1), it is considered good practice to obtain written consent from the owner of personal data, even if some sector-specific laws do not require it, in order to guarantee the respect of the right to informative-auto determination.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The violation of privacy could be sanctioned, if the violation is recognized by a Judge as a criminal offence under the Criminal Code, with imprisonment of 1 to 5 years (in case of computer data manipulation) or fines (in case of alteration, access and misuse of data or of data manipulation).

10.2 Do individuals have a private right of action? What are the potential remedies?

Individuals have a general private right of action to claim compensation for non-material damage caused by wrongful data processing. Potential remedies could be economic compensation for the damage caused.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Bolivia which affect privacy?

No, Bolivian culture has no particular rules that could affect privacy.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

A draft bill was presented to the lower chamber of the Bolivian Assembly on November 30, 2018, although this law has not, as yet, been passed.

This draft legislation includes the principles developed by the Inter-American Juridical Committee (see question 3.3), together with all other previously mentioned legal provisions; and establishes the obligation on companies, or any person who is processing personal data, to implement appropriate mechanisms to prove compliance with its obligations regarding protection of personal data.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Bolivia?

Currently, Bolivia has not developed specific regulations related to data protection. However, since the basis of data protection has been recognized by the Bolivian Constitutional Court, we advise, to avoid future claims, the implementation of general principles and international good practices regarding data protection.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Over the past few years, privacy regulation has been significantly developed through national and international legislation. There is a new dimension to already-existing rights, that is a logical response to the impact of new technologies in everyday life and the commercial opportunities that they represent. The development of these rights has created new obligations on companies, which affect their interaction with costumers and the public in general.

These changes have been triggered by the new channels of interaction that the new technologies have created between persons and companies, and the new necessities they bring.

12.2 What do you envision the privacy landscape will look like in 5 years?

In five years, the extent of privacy as a right will be better understood by people and companies, and the rules of interaction through new technologies will be clearer. By having a better understanding of the rules applicable to privacy, companies and their customers/consumers will be able to take advantage of new technologies within the scope of these rules. Companies must face the challenges that arise with the development of privacy in order to meet their consumers' demands, and, in the long term, this will generate new commercial interaction.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Currently, companies are compelled to include new mechanisms to ensure correct data processing. These new mechanisms should include procedures to ensure informed consent and guarantee the security of this information, and other channels to comply with the new obligations on companies. Companies must adapt their structures and internal regulation to meet these standards.

Additionally, companies must have a procedure to solve any problems related to data protection. New technologies represent a new, faster and easier medium to transfer information; and companies must be prepared to face any conflict that could result from a misuse of personal data in this medium, when errors cannot be avoided.

BRAZIL

1 PRIVACY LAW

1.1 How is privacy regulated in Brazil?

The Brazilian Constitution stablishes general principles that protect the privacy and confidentiality of personal information and communication. Accordingly, it provides for the inviolable right to intimacy, privacy, honor and image of individuals (article 5, item X). The Constitution also provides for the confidentiality of correspondence and telegraphic communications, data and telephone communication (article 5, item XII). Violation of the above rights entitles the individual to indemnification for moral or material damages (article 5, item X).

The Civil Code does not define privacy, but provides that the private life of an individual shall not be violated and that the judge shall, upon request of the interested party, take the necessary measures to stop or to impede any act contrary to this rule (article 21). The Civil Code further states that the right to privacy is a personal right, which cannot be waived or assigned (article 11).

Moreover, the Brazilian General Data Protection Law ("LGPD"), the first specific legislation on the subject in Brazil, was signed into law on August 14, 2018. The text follows the worldwide trend of strengthening personal data protection, guaranteeing a series of rights to data subjects, as well as imposing important obligations on processing agents. The LGPD replicates key points of the European General Data Protection Regulation ("GDPR"). This new law will be effective as of August 2020.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Although the LGPD (Federal Law 13,709/18) is not effective yet, the Brazilian legislation has other norms currently in use for the control of the use of personal data for advertising. The most important laws used in these cases — concerning topics from image rights to rights of information and transparency of services — are:

(a) The 1988 Federal Constitution;

(b) The Brazilian Civil Code (Federal Law 10,406/02);

(c) The Consumer Defense Code (Federal Law 8,078/90);

(d) The Brazilian Civil Framework of the Internet (Federal Law 12,965/14, complemented by Decree 7,724/12);

(e) The Child and Adolescent Statute (Federal Law 8,069/90);

(f) Bank Secrecy Law (Law 105/01);

(g) Telephone Calls Interception Law (Law 9,296/96);

(h) Public Information Access Law (Law 12,527/11; complemented by Decree 7,724/12);

(i) Cyber-Security Policy (Resolution 4,658/2018 by the Brazilian Central Bank);

(j) Habeas Data Law (Law 9,507/97); and

(k) Nonpayers' Register Law (Law 12,414/11).

The LGPD also establishes the National Data Protection Authority ("ANPD"), responsible for overseeing, implementing and enforcing LGPD compliance. See question 1.3.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

In addition to the regular courts, which are responsible for civil and criminal lawsuits, the ANPD, established by the LGPD (through Provisional Measure 869) is responsible for overseeing, implementing and enforcing LGPD compliance.

The Provisional Measure establishes, among other things, that the ANPD is an agency with technical and decision-making autonomy and is of a transitional legal nature, which can be transformed into an indirect federal public administration entity within two years.

The ANPD is to:

(a) develop guidelines for the National Policy of Personal Data and Privacy, as well as specific rules;

(b) coordinate its activities with regulators of specific sectors, to ensure the fulfilment of their duties with the greatest efficiency;

(c) disseminate in society information about the norms and public politics of protection of personal data and about measures for security; and

(d) have exclusive competence to apply sanctions.

These powers should take precedence over those of other public administration entities.

The ANPD is still in process of formation.

2 SCOPE

2.1 Which companies are subject to privacy law in Brazil?

The LGPD is applicable to any company whenever personal data is collected from individuals located in Brazil, the processing is performed in Brazil, or there is the offer of goods and services to individuals located in Brazil.

However, it is not applicable for:

(a) public security,

(b) data coming from and destined for other countries that is only in transit through Brazil,

(c) personal or non-commercial use, and

(d) journalistic, artistic or academic purposes.

2.2 Does privacy law in Brazil apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The LGPD establishes the principle of extraterritoriality in its application. As a result, the new rules apply not only to companies located in Brazil, but also to entities that process or collect data in the Brazilian territory and to companies that aim to offer or supply goods and services to individuals located in Brazil.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Brazil?

According to the LGPD, "Personal Data" is information related to a natural persona who is directly identifiable by that information or can be possibly identified from it.

Personal data must have been collected on national territory to comply with the law.

For each type of data, the LGPD reserves a different model of conduct to be adopted during processing, with limitations on the assumptions in which personal and sensitive data may be processed (see question 3.2).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Data processing follows different rules depending on the type of data we are dealing with. Data may be divided in two major groups:

(a) In the first, there are two types of data that we need to be careful about:

(i) Anonymized data — which is data that does not contain the data subject's identification element and will only be considered personal data when the anonymization process to which it was submitted is reversed or can be reversed; and

(ii) Pseudonymized data — which is data that has encrypted identification elements and where reversibility is possible.

(b) In the second group, there are two types of data to which the LGPD grants greater protection:

(i) Personal data — information related to the identified or identifiable natural person (including identifying numbers, location data or electronic identifiers, when these relate to a person); and

(ii) Sensitive personal data — information such as racial or ethnic origin, religious beliefs, political opinions, membership of trade unions or religious, philosophical or political organizations relating to health or sexual life, genetic or biometric data, etc.

Personal or sensitive data processing is allowed in the following exceptional cases:

- for the fulfilment of a legal or regulatory obligation;
- by the public administration, for the implementation of public policies established by law;
- for the conduction of studies by research bodies, provided that anonymity is maintained;
- for the performance of the contract to which the data subject is party;
- for the regular exercise of rights in judicial, administrative or arbitral proceedings;
- for the protection of the data subject's or third party's life or physical integrity;
- for health protection, with procedures performed by health professionals or health entities;
- for the protection of credit, under the terms of the Consumer Defense Code; and

- when it is necessary to meet the legitimate interests pursued by the controller (ie, the individual or legal entity which is responsible for making decisions regarding the processing of data) 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).

Aside from the above-mentioned exceptions, the processing agents must obtain the freely-given, informed and unambiguous consent of the data subject, in writing or by other means that indicate the data subject's agreement, both to the data processing and to the sharing of the data with other companies. The data subject may withdraw such consent at any time.

The use of children's or teenagers' data must be made with specific consent given by at least one parent or legal guardian. Personal data of minors may be collected without this consent when collection is necessary to contact the parent or legal guardian, when it is used only for storage purposes, or for the minor's protection, and in no case may be passed on to a third party without the consent of at least one parent or legal guardian. Controllers may not restrain the participation of minors in games, internet applications, or other activities to the provision of personal information beyond what is strictly necessary for the activity. The controller must also make reasonable efforts to verify that consent has been given by the child or teenager concerned, considering available technologies, and to ensure that data processing information is provided in a simple, clear and accessible manner, taking into account the intellectual and mental aspects of the user, with the use of audiovisual resources when appropriate, in order to provide the necessary information to the parents or legal guardian, and adequate to the understanding of the child or teenager.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The ten principles that companies need to follow regarding the processing of personal data are:

(a) Purpose — Legitimate, limited, explicit and informed purposes for processing;

(b) Adequacy — Compatible with the purposes;

(c) Necessity — Use of data only when necessary;

(d) Free access — Provision of free and integral access to data subjects on the processed data;

(e) Quality of data — Accurate, clear and updated data;

(f) Transparency — Clear and accurate information to data subjects;

(g) Security — Effective technical and administrative measures regarding data protection;

(h) Prevention — Adoption of measures to avoid damage to data subjects, such as periodic diligence, training etc;

(i) Non-discrimination — No use for discriminatory purposes; and

(j) Liability and accountability — Evidence of effective measures for compliance with the LGPD.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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

(a) The Processor — a natural or legal person, under public or private law, who processes personal data on behalf of the controller;

(b) The Controller — a natural or legal person, whether public or private, who takes the decisions concerning the processing of personal data; and

(c) The Data Protection Officer ("DPO") — a natural or legal person, appointed by the controller, who acts as a communication channel between the controller and the data subject and the competent authority.

If the controller or the processor (together, the "processing agents"), due to the exercise of the activity of processing personal data, causes property, moral, individual or collective damage to others, in violation of the legislation on protection of personal data, he is obliged to redress it.

In order to ensure effective compensation to the data subject, the LGPD provides joint liability in cases when (i) the damage was caused by processing made by the processor after breaching the data protection law obligations, or (ii) he has not followed the controller's lawful instructions; and when the controller is directly involved in the treatment which caused the damage.

However, the processing agents will not be held responsible when they prove: (i) that they have not processed the personal data; (ii) that, although they have processed the personal data, there has been no violation of data protection legislation; or (iii) that the damage was caused by the data subject or a third party's fault.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The processing agents — or any other person who intervenes in one of the processing phases — are required to ensure the security of the personal data information, as provided in the LGPD, even after the completion of the processing.

The processing agent 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 or identification of the controller.

The processor must process the data according to the instructions provided by the controller, who will verify compliance with the instructions and the rules on the matter.

The controller and the processor must keep a record of the personal data processing operations that they perform, especially when based on legitimate interest.

The ANPD may require the controller to draw up a report on the impact on the protection of personal data, including sensitive data, regarding its data processing operations, under the terms of the regulation, subject to commercial and industrial secrets. This report must contain, as a minimum:

- a description of the types of data collected,
- the methodology used for the collection and for ensuring the security of the information, and
- the controller's analysis regarding the measures, safeguards and risk mitigation mechanisms adopted.

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. The activities of the DPO consist of:

- receiving complaints and communications from data subjects, providing clarification and adopting measures to solve these;
- receiving communications from the ANPD;
- advising the entity's employees and contractors regarding the practices to be taken in relation to the protection of personal data; and
- performing other duties as determined by the controller or as set out in complementary rules.

Note that the ANPD may establish complementary rules concerning the definition and duties of the DPO, including situations in which the need for his appointment is exempted, according to the nature and size of the entity, or the volume of the data processing operations.

Except in specific situations, the 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 agent will not delete the personal data after the end of its processing are:

- for compliance with legal or regulatory obligation by the controller;
- for study by research body, ensuring, whenever possible, anonymization of personal data;
- for transfer to a third party, provided that the data processing requirements laid down in the LGPD are respected; or
- for exclusive use of the controller, as long as it is anonymised, being forbidden its access by a third party.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Brazil? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security for the processing of personal data shall be structured to meet security requirements, the governance standards, and the general principles set forth in the LGPD and in other laws (see, further, question 1.2).

Please note that it is part of the ANPD's responsibility to oversee, implement and enforce privacy compliance. Thus, it is expected that new regulations be drafted in the near future.

6.2 How are data breaches regulated in Brazil? What are the requirements for responding to data breaches?

The Brazilian Civil Framework of the Internet provides for the right of inviolability of privacy of the Internet user, ensuring compensation for material or moral damage arising from its violation.

The LGPD provides that the controller must report to the ANPD and to the data subject the occurrence of a safety incident that may lead to significant risk or damage to the data subject. The communication should be made within a reasonable period of time, as defined by the ANPD, and should mention at least:

(a) the description of the nature of the affected personal data;

(b) information about the data subjects involved;

(c) indication of the technical and security measures used for data protection, observing the trade and industrial secrets;

(d) the risks related to the incident; the reasons for the delay, in case the communication was not immediate; and

(e) the measures that have been or will be taken to reverse or mitigate the effects of the damage.

The ANPD will verify the seriousness of the incident and may, if necessary to safeguard the rights of the data subjects, order the controller to adopt measures such as wide dissemination of the fact in the media and measures to reverse or mitigate the effects of the incident. During its judgment as to the severity of the incident, it will evaluate whether there is any evidence that appropriate technical measures have been taken to render the affected personal data unintelligible to third parties not authorized to access them.

For more information on the penalties, please see question 10.1.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The LGPD guarantees a wide range of rights to data subjects, such as:

(a) confirmation of the existence of processing;

(b) access to their data;

(c) correction of incomplete, inaccurate or outdated data;

(d) anonymization, blocking or elimination of unnecessary, excessive or treated data in breach of the law;

(e) portability of the data to another service or product provider, upon express request and observing the commercial and industrial secrecy, according to the guidance of the data protection authority;

(f) elimination of personal data processed with the consent of the data subject, except in the cases provided for by law;

(g) information on public and private entities with which the controller promoted shared use of data;

(h) information about the possibility of not providing consent and the consequences of the refusal; and

(i) withdrawal of consent at any time.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

This type of marketing falls under general privacy and advertising regulations set out in the LGPD, the Brazilian Federal Constitution, the Brazilian Civil Code, the Brazilian Consumer Defense Code, the Brazilian Advertising Self-Regulation Code, and other laws mentioned in question 1.2.

It is worth noting that the Brazilian Superior Court of Justice has ruled that the making of certain telephone calls for marketing purposes to a consumer at home or work with coercive or dishonest business methods, without the consumer's approval, is deemed "abusive publicity" and, therefore, illegal (article 6, item IV, of the Consumer's Defense Code).

Thus. it is recommended that companies obtain the consumer's express consent before making telephone calls for marketing purposes (based on the opt-in system).

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There are no specific privacy rules governing tracking technologies, although the privacy rules contained in the LGPD and other laws mentioned in question 1.2 must be respected.

The expectation is that the ANPD will issue rules that will cover the specific points not yet regulated.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There are no specific privacy rules governing targeted advertising and behavioral advertising, although they the privacy rules contained in the LGPD and other laws mentioned in question 1.2 must be respected.

The expectation is that the ANPD will issue rules that will cover the specific points not yet regulated.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

No personal data may be transferred to third parties, including access logs and connection logs, unless the user consents or it is allowed by law. The LGPD provides for the principle of transparency in the processing of personal data. This means that the data subject must have clear, accurate and easily accessible information about who is handling their data. Accordingly, in the event that a controller, who has obtained the consent of the data subject for the processing of his data, needs to communicate or share personal data with other controllers, he must obtain the specific consent of the data subject for that purpose. In practice, if the controller needs to transfer the collected data to third parties, data

subjects should have clear information about such transfer, for example through the controller's privacy policy. Additionally, if the controller processes the data based on the consent of the data subject, there must be specific consent of the data subject to the transfer.

8.5 Are there specific privacy rules governing data brokers?

There are no specific privacy rules governing data brokers, although the privacy rules contained in the LGPD and other laws mentioned in question 1.2 must be respected.

The expectation is that the ANPD will issue rules that will cover the specific points not yet regulated.

8.6 How is social media regulated from a privacy perspective?

There are no specific privacy rules governing social media, although the privacy rules contained in the LGPD and other laws mentioned in question 1.2 must be respected.

The expectation is that the ANPD will issue rules that will cover the specific points not yet regulated.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

In addition to the laws mentioned in question 1.2, loyalty programs and promotions are also regulated by:

(a) The Consumer Defense Code — This law establishes the legal principles and requirements applicable to consumer relations in Brazil. It regulates, among other things, product and service liability, contractual clauses, commercial practices, advertising and relevant information on products and services offered to consumers. Misleading and abusive advertising are strictly prohibited. In addition, according to the Consumer Defense Code, the opening of registration, form, registration and personal and consumer data must be communicated in writing to the consumer, when not requested by him.

(b) Brazilian Advertising Self-Regulation Code ("Self-Regulation Code") — Any activity designed to stimulate the consumption of products and services and promote institutions, concepts or ideas is considered to be advertising and subject to the rules of the Self-Regulation Code. Although the Self-Regulation Code is not enshrined in law, on the few occasions when the Self-Regulation Council's rulings have been challenged in a court of law, its decisions have prevailed. As a result, the Self-Regulation Code is also used as a reference document and considered subsidiary legislation by Brazilian courts.

(c) Decree Law 70,951/72 and Law 13,756/2018, regulating Law 5,768/71 — Under this, all promotions involving the free distribution of prizes (contests, sweepstakes and gift certificates) require the authorisation of the Fiscal, Energy and Lottery Secretariat, which is linked to the Ministry of Economy, the Brazilian National Savings Bank before being implemented in Brazil.

(d) Decree Law 7,962/2013 ("Electronic Commerce Decree") — This Law regulates consumer relations on the internet and includes applicable provisions.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

As to transfer of data generally, see question 8.4.

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 this Law, in the form of:

  (i) specific contractual clauses for a given transfer,

  (ii) standard contractual clauses,

  (iii) global corporate standards, or

  (iv) 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 national authority 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Please see question 9.1.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

In addition to damage to the company's reputation in the public eye, the LGPD provides for the following legal penalties:

(a) warnings;

(b) obligation to disclose the incident (see, further, question 6.2);

(c) data deletion;

(d) fines of up to 2% of business group revenues in Brazil, limited to R$ 50,000,000.00 per infraction;

(e) daily fine of up to R$ 50,000,000.00 per infraction; and

(f) data lock.

10.2 Do individuals have a private right of action? What are the potential remedies?

Individuals have a private right of action by bringing civil and criminal lawsuits before the regular courts, on the basis of the laws mentioned in question 1.2.

The lawsuits may result in compensation for material and moral damages.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Brazil which affect privacy?

There are no rules particular to the culture of Brazil.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Companies must be aware of the LGPD — which will be effective as of August 2020 — and of regulations that will be issued by the ANPD.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Brazil?

There is no additional relevant information.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Due to globalization, the recent technological developments, and the advent of social media, human beings all around the globe have begun to produce and share massive amounts of data on a scale that has never been seen before. These great alterations on everyday life have resulted in the rise of major scandals — in particular, the best known of all: the Facebook–Cambridge Analytica data scandal. These scandals have led to a realization of the danger that this unregulated sector represents to individuals privacy safety and for society as a whole — finally leading citizens to demand stronger laws to deal with this issue.

12.2 What do you envision the privacy landscape will look like in 5 years?

In five years, with the raising of awareness of the importance of personal data and a greater demand for government action, regulation should become increasingly clear and comprehensive, securing to individuals greater rights and transparency in the use of their data.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Private companies have the period until the LGPD comes into force (August 2020) to adapt their current systems. It is recommended to update companies' terms of use and privacy policies and to seek the data subject's specific consent for the data previously collected to proceed properly with the data treatment. Companies will need to keep up with the many changes that will happen in the near future, looking for the assistance of specialized professionals.

CANADA

1 PRIVACY LAW

1.1 How is privacy 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

In Canada, there is both federal and provincial privacy legislation governing the collection, use, disclosure and management of personal information:

(a) **Personal Information (Federal):** 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) **Personal Information (Provincial)**: 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 are subject to:

  (i) Personal Information Protection Act (British Columbia),

  (ii) Act Respecting the Protection of Personal Information in the Private Sector (Quebec), or

  (iii) Personal Information Protection Act (Alberta),

  rather than PIPEDA.

(c) **Health and Employment Personal Information (Provincial)**: Certain provinces also have privacy legislation in place for health (Ontario, New Brunswick, Newfoundland and Labrador, Nova Scotia) and employment (Alberta and British Columbia) personal information.

For the purposes of this chapter, we will focus on the privacy legislation in (a) and (b), referred to herein 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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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. In each of these provinces, the regulator is known as:

(a) Alberta: Office of the Information and Privacy Commissioner;

(b) Quebec: Commission d'accès à l'information du Québec;

(c) British Columbia: Office of the Information and Privacy Commissioner for British Columbia.

2 SCOPE

2.1 Which companies are 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. Some organizations regulated federally from a constitutional perspective are not subject to provincial private sector privacy legislation.

2.2 Does privacy law in Canada apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Privacy law applies to organizations conducting business in Canada that handle the personal information of Canadians. If a non-Canadian organization does business in Canada and collects, uses or discloses personal information of a Canadian, 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 INFORMATION

3.1 How is personal information/personal data defined 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 identify an individual. In the legislation:

(a) PIPEDA: "Personal information" means information about an identifiable individual.

(b) Quebec: "Personal information" is any information which relates to a natural person and allows that person to be identified.

(c) Alberta: "Personal information" means information about an identifiable individual.

(d) British Columbia: "Personal information" means information about an identifiable individual and includes employee personal information but does not include (i) contact information, or (ii) work product information.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive personal information/personal data" is not defined in any Canadian privacy legislation. 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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The key privacy principles work in unison and are as follows:

(a) **Consent**: Organizations must obtain meaningful consent when collecting, using or disclosing personal information. PIPEDA requires that it would be reasonable to expect that individuals would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. For consent to be valid, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner. This is typically achieved with a privacy policy. The type of consent required (express or implied) will depend on the following factors:

(i) Nature of the information: Sensitive personal information will most often require an individual's express consent.

(ii) Reasonable expectations: If there is a use or disclosure that an individual would not expect in the circumstances (eg, transfer to third party; location tracking), express consent is required.

(iii) Risk of harm: If there is a material risk of harm to an individual that could arise from the collection, use or disclosure of his/her personal information, express consent is required.

(b) **Identifying Purposes**: Organizations must identify the purposes for which the personal information is collected, either before or at the time of collection.

(c) **Accountability**: Organizations are responsible for personal information under their control, including when it is transferred to a third party for processing. Organizations must also designate an individual (eg, a privacy officer) who will be responsible for the organization's privacy compliance as well as handle consumer complaints and requests.

(d) **Limiting Use, Collection, Disclosure and Retention:** Collection of personal information should be limited to that which is necessary to fulfil the intended purpose. Also, the information should be retained only for as long as is necessary for the fulfilment of the purpose(s) stated at the time it was collected.

(e) **Security**: Personal information must be protected by security safeguards appropriate for the sensitivity of the information. These safeguards must protect against loss, theft and unwanted disclosure.

(f) **Openness:** Organizations must document, and make readily available to individuals, specific information about their policies and practices relating to the handling of personal information.

(g) **Accuracy:** Organizations have an obligation to ensure that personal information in their records is accurate, complete and up-to-date, as necessary for the identified purposes.

(h) **Access:** Individuals have a right to access the personal information that an organization holds about them and to request that inaccuracies in the information be corrected or noted.

(i) **Recourse**: Organizations must develop simple and easily accessible complaint procedures.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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. 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

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) notify the regulator of a data breach.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Canada? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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.

6.2 How are data breaches regulated in Canada? What are the requirements for responding to data breaches?

(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". 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 the following:

(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.

"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 the personal information has been or will be misused.

(b) In Alberta, an organization must notify the Information and Privacy Commissioner of Alberta without unreasonable delay of a breach where there is a real risk of significant harm to individuals. The notice must be in writing and include similar details as those required by PIPEDA in (a) above.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

An individual has the following rights:

(a) to request access to the personal information an organization holds about him/her;

(b) to request the correction of the errors or inaccuracies of his/her personal information;

(c) to withdraw consent at any time. The individual must be informed of the implications associated with the withdrawal; and

(d) to complain to the relevant privacy authorities.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The information collected by this technology is likely classified as personal information and is subject to PIPEDA. The type of consent required (implied or express) will depend on the sensitivity of the information collected and the reasonable expectations of the individual. See also question 8.3, as cookies, pixels and SDKs are often used in online behavioral advertising.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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). 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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The type of consent required (express or implied) will depend on the sensitivity of the personal information collected, as well as the reasonable expectations of the individual.

8.5 Are there specific privacy rules governing data brokers?

No. However, any sale or other disclosure of personal information to a third party would likely require express consent from the affected individuals.

8.6 How is social media regulated from a privacy perspective?

Social media is not treated differently, and organizations hosting or participating on social media platforms are subject to Canadian privacy legislation in the same manner as other organizations.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Yes, 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".

Further, in Alberta, if an organization uses a service provider outside of Canada to collect, use, disclose or store personal information, it must disclose (eg, in their 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Companies should, in order to be transparent in their handling of personal information, advise customers that their personal information may be sent to another jurisdiction for processing, and that it may be accessed by the courts, law enforcement and national security authorities while it is in another jurisdiction.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

(a) **Data security**: Under PIPEDA, failure to comply with the breach notification provisions is an offence punishable on summary conviction with a fine not exceeding $10,000, or, as an indictable offence, a fine not exceeding $100,000.

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 $10,000, in the case of a person other than an individual, to a fine not exceeding $100,000.

(b) **Privacy**: 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.

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 $10,000 for an offence punishable on summary conviction or $100,000 for an indictable offence.

10.2 Do individuals have a private right of action? What are the potential remedies?

There is no private right of action. However, there are growing common law causes of action for invasion of privacy in some Canadian provinces. These torts could 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Canada which affect privacy?

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 his/her private life. It is important to note that the Quebec Charter applies to all disputes, whether or not they involve government action.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The OPC recently initiated a consultation to consider its position on cross border data transfers under PIPEDA. In particular, it considered imposing a requirement that such transfers take place only with the consent of the data subject. This would have been a significant change. Since 2009, the OPC has held that businesses transferring personal information to service providers outside of Canada for processing are required to provide notice to individuals and to ensure, through contractual or other means, that the data recipient will provide a comparable level of protection while the information is being processed by the service provider. The OPC does not require the individual's express consent for the data transfer, provided that the "use" of the personal information was for the purpose for which it was originally collected.

On September 23, 2019, the OPC announced that it had concluded its consultation on cross border data transfers and that its guidelines for processing personal data across borders will remain unchanged, for now.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Canada?

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.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Over the years, the concept of consent has seen some of the biggest changes in the privacy landscape in Canada. The scope and application of consent has been constantly adapting to the evolution of big data practices and individuals' sophistication regarding the value of their personal information — and purposes for which it is used. The evolution of consent has also been reflected in expanding the regulatory interpretation of existing legislation and enforcement approaches. For example, the recently concluded federal regulatory consultation suggests that the OPC may take the position in the near future that the cross-border flow of data will require an elevated form of consent (see question 11.2).

Another significant change to the privacy landscape in Canada is the ubiquitous use of technology in daily transactions and interactions, and the speed with which platforms facilitating data exchange have continued to evolve. While data practices become increasingly more sophisticated, regulatory views on the "reasonable expectations" of Canadians has not kept up. Multi-page privacy policies with complex terminology are no longer sufficient to provide appropriate disclosure of a business' privacy practices and establish the sole basis for informed consent.

12.2 What do you envision the privacy landscape will look like in 5 years?

As individuals are becoming more aware of the value of their data, organizations will need to be prepared for more questions, transparency and, possibly, complaints. The common law causes of private action will become more significant legal and practical risks to organizations. It is likely that there will be a significant legislative reform at the federal level in the next 5 years, driven by changing legislative regimes internationally, and reflected in the stated priorities of the federal government prior to its 2019 re-election.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Meaningful consent and data security are the key privacy challenges for organizations. Explaining the proposed use of an individual's personal information in way that he/she can understand is key to establishing meaningful consent at law. As technologies and processes evolve, organizations are facing increasing challenges in translating the complexity of their use of data to everyday Canadians in a simple, yet meaningful, manner.

Further, the value and quantity of personal information being exchanged, particularly across borders, has resulted in the rise of significant data breaches in Canada, including those involving personal financial information. 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.

CHILE

1 PRIVACY LAW

1.1 How is privacy regulated in Chile?

In Chile, privacy is regulated mainly by Law 19.628, "On the protection of private life", commonly referred as "the Personal Data Protection Law" ("DPL"). It dates from 1998, 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 1998, the law has undergone some minor changes, which are mostly related to the transfer of debtor lists and the criteria of commercial risk assessments.

Nevertheless, the most commonly used way of exercising rights over personal data is through constitutional actions. In 2018, this was consolidated by incorporating into the constitutional text the protection of personal data, identifying such right separately to the right of privacy.

A new Data Protection Bill is currently being debated in the Chilean Congress, which is inspired by the GDPR.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Data protection is addressed in several specific laws, as well as provisions scattered in related or complementary laws and other legal authority. The main laws and decrees containing data protection provisions are:

(a) Constitution of the Republic of Chile, Article 19(4): establishes the right to "the respect and protection of private life and the honor of the person and his 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.

(b) DPL: mainly defines and refers to the treatment of personal information in public and private databases.

(c) Law 20,285, "On the Access to Public Information": sets forth the public function Transparency Principle, ie, an individual's right to access the information held by public administration bodies, and the procedures and exceptions thereof.

(d) General Law on Banks, Article 154: establishes banking secrecy. It provides that, subject to certain specific exemptions, all deposits are secret, and account-related information can be given only to the account's owner or designated representative.

(e) Law 19,223, "Criminal Conducts related to Informatics": establishes sanctions for those who breach and unlawfully access and/or use information available in electronic databases.

(f) Decree No 13 of 2009, Ministry of the General Secretary of the Presidency: establishes the Rules (or administrative provisions and procedures) of Law 20,285.

(g) Decree No 779 of 2000, Ministry of Justice: establishes the Rules of the personal databank of Public Entities which provide that the Civil Registry and Identification Service will manage public databanks on behalf of all public bodies.

With a special focus on advertising aspects, there is a self-regulatory body called the Association of Direct and Digital Marketing of Chile AG, which enforces the Code of Ethics and Self-regulation of the Direct and Digital Marketing Association of Chile AG". This Code has an annex called the Recommendations of the Self-Regulation Council of Direct and Digital Marketing on Consumer Rights in the Processing of their Personal Data", in which recommendations regarding six topics are made:

- Principles of data processing,
- Consumer consent for data processing,
- Consumer rights in data processing,
- Responsibility and governance in data processing,
- Security in data processing, and
- Processing of personal data by third parties.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The remedy set out in the DPL is the *habeas data* action, whereby the data subject can apply to the person in charge of a databank with a request for information, or for information to be corrected, updated or deleted. Where the person in charge of the databank does not rule on such request within two business days, or when it is denied, the person can go to court, which must proceed with the request through a brief and summary procedure. If the claim is accepted, the judge will set a reasonable period of time to comply with the decision and may apply a fine of one to ten monthly tax units (US $70–700), or ten to fifty monthly tax units (US $700–4000, approximately) if the data were related to obligations of an economic, financial, banking or commercial nature.

However, those who are victims of an illegitimate treatment of their data rarely execute the *habeas data* action available in the law, 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 the Chilean Court of Appeals 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).

Regarding public data processing, Law No 20,285 granted the Chilean Council for Transparency the competence to ensure adequate compliance with the DPL regarding the protection of personal data by the organs of the State Administration. Unfortunately, it was not granted the ability to sanction breaches of certain obligations, so the lack of compliance with the provisions of the law indicated by public bodies has not been mitigated.

2 SCOPE

2.1 Which companies are subject to privacy law in Chile?

All companies are subject to privacy law in Chile, including both those in the private and public sectors. There are no excluded industry sectors.

2.2 Does privacy law in Chile apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No, unlike the GDPR, there are no explicit extraterritorial dispositions in Chilean privacy law.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Chile?

"Personal data" is defined as "any data related to information of any type concerning identified or identifiable natural persons".

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The 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 DPL was drafted.

Sensitive data may not be processed, unless there is legal authorization, the data subject has consented, or the sensitive data is necessary to grant healthcare benefits to its holder. In practice, there are fewer exceptions available to process sensitive personal data than regular personal identifiable information, which translates into companies relying on individual consent in order to lawfully process this information.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

In Chile, the principles of data protection are not expressly established in legislation, however they are understood to be incorporated in the norm through legal interpretation of the DPL's main provisions:

(a) Lawfulness and fairness: which means treating the data in accordance with the law and respecting the authorization of the owner;

(b) Purpose Limitation: which mandates that personal data can only be used and processed for the purposes for which they were collected;

(c) Storage limitation: that is, to treat the data only until the purposes of the treatment have been fulfilled, storing it only for the sufficient time;

(d) Principle of Accuracy: that is, that data must be accurate, up-to-date, and accurately reflect the real situation of its owner; and

(e) Integrity and confidentiality: the obligation of the controller of personal data to take care of it with due diligence, taking responsibility for the damages caused.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The DPL does not use the term "controller" which is present in other jurisdictions. Rather, the DPL considers the role of "responsible person" which is accountable for mitigating harm or damage to an individual as a result of processing their personal data. The "responsible person", ie, the natural person, legal entity or public body that makes decisions related to the use of personal data, is responsible for ensuring that personal data is protected in accordance with applicable law. The general duty of care that the law imposes is that of "due diligence".

The DPL addresses the role of "data processor" when the processing of private databases is delegated to a third party. In these instances, the DPL mandates that the contract between both parties must be in writing and include the conditions stipulated in the processing.

There are no additional explicit provisions on the responsibilities or definitions of these two roles.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Regarding advertising, the most relevant obligation lies in the Chilean consumer law, which establishes the right to receive truthful and timely information about the goods and services offered, their price, contracting conditions and other relevant characteristics thereof, which pushes companies to generate provisions regarding data protection in their terms and conditions, or, properly, a privacy policy.

Among other obligations that the "responsible persons", or "controllers" as this role is described in other jurisdictions, must fulfil, it is to maintain the quality of the data so that the available information is accurate, updated, and truthful regarding the real situation of the data owner. The controller must also maintain the security of the data, taking care of the data with due diligence. Moreover, there is a duty of secrecy on those in charge of the records, which is not extinguished by having ceased activity as manager.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Chile? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is briefly regulated in the current DPL. The DPL establishes that all personnel involved in personal data processing have a legal obligation of confidentiality related to data that is not publicly available, even after the end of their contractual relationship. The security of personal data contained in databases is an obligation of the controller (or "responsible person", as it's called in the DPL). The responsible person must maintain the database, and keep it "with due diligence, being held accountable for the damages."

The banking industry has some specific regulations concerning data security, being the obligation to identify, record, evaluate, control, mitigate, monitor, and report operational incidents. The bank, in case of incident, will be responsible for keeping the Superintendency informed of the situation under development and the measures or actions for detection, response, and recovery of the incident.

The information must be sent to the extranet account enabled by the authority, at any time, both working and non-working days, within a maximum period of 30 minutes after its occurrence. The information must be reported at the start and at the time of closing the incident, including basic data of the reporting entity and of the incident.

If the incident affects the quality or continuity of services to clients, or is a fact of public knowledge, the institution will be responsible for informing users promptly about the occurrence of the event.

6.2 How are data breaches regulated in Chile? What are the requirements for responding to data breaches?

Current legislation does not establish universal standards or measures that must be taken with respect to data breaches. Therefore, if there is a data breach and that breach causes damage to a data subject, compensation for that damage must be obtained through normal civil procedures. Exceptionally, the banking and finance sectors have established some regulatory norms in relation to cybersecurity, which may involve personal data breaches, but these are focused on the security of the information, regardless of its nature.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Chilean law explicitly recognizes the following data subject rights, which are collectively referred as "ARCO" rights after their initials in Spanish (*acceso, rectificacion, cancelacion and oposicion*):

(a) **The right to be informed**: Prior to giving consent, the data subject must be informed of the purpose of the data processing and whether the data will be made publicly available.

(b) **The right to data access**: The data subject can request, free of charge, access to her/his personal data, as well as information about the sources and recipients of such data, the purpose of the processing, and the identity of third parties to whom that data is being transferred to regularly.

(c) **The right to rectify data**: If data is wrong, inaccurate, or incomplete, the data subject may request the modification of such data.

(d) **The right to eliminate or block data**: If the personal data is not stored legally (eg, no consent was obtained) or if the data is no longer up-to-date or the authorization to process the data has expired, then the data subject will be able to request that the person in charge of the database delete his/her data from it. Data subjects also have the right to request the deletion of or block on personal data stored in a database, if such data was given voluntarily by the data subject, or if the data is being used to send marketing communications.

Data subjects can exercise these rights free of charge, every six months.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications is one of the exceptions considered in the DPL to the processing and use personal data in the absence of explicit consent by the data subject. If the personal data is obtained from a publicly available source and the data is needed to provide direct commercial communications, then individual consent is not required.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Tracking technologies is not explicitly addressed in the DPL. Furthermore, geo-localization data is not mentioned in the law, although it can be understood to be considered to be sensitive data. Consequently, following the general data protection rules, to lawfully use data collected by tracking technologies, explicit consent must be obtained from the data subjects.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted and behavioral advertising are not explicitly mentioned or addressed in current law. Consequently, following the DPL general rules, personal data that is collected for the purposes of targeting must be obtained either through a publicly available source or with the explicit consent of the data subject. Data subjects can exercise any of their ARCO rights, particularly the right to eliminate or block data, if it is being used for purposes of marketing communications.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Unless the data has been obtained from a publicly available source, advertisers need to ensure that data subjects have been informed of the purpose of the data collection (customer matching) and secure explicit consent to process such data for that purpose.

8.5 Are there specific privacy rules governing data brokers?

No, there are no specific rules in relation to data brokers. Consequently, the general rules, rights and principles outlined in questions 7 and 3.3 will apply.

8.6 How is social media regulated from a privacy perspective?

Advertising campaigns made through social media need to follow the general rules, rights and principles outlined in questions 7 and 3.3.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs and promotions need to follow the general rules, rights and principles outlined in questions 7 and 3.3.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Transborder data transfer is not explicitly regulated in the DPL. Consequently, any transfers of personal data outside the country, including transfer between group of companies, follow general rules. In practice, companies should ask for consent from data subjects to transfer their data outside of Chilean borders.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Since there are no provisions regarding cross-border transfer of data, there are no special issues to be considered.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The current Chilean law on data protection is characterized by the lack of sanctions and effective penalties for breaches of the obligations required by law; the only existing sanctions in the DPL are those awarded after a judicial determination of breach of *habeas data*, ranging from USD $70–4,000, being meager penalties.

Without prejudice to this, data subjects have the right to request compensation in a civil court, whether for direct or even moral damage, for the infringements of their rights by the controller.

10.2 Do individuals have a private right of action? What are the potential remedies?

In the Chilean system, individuals may bring private actions for breach of privacy; however, these are not special rights, and are regulated by the general civil law, by a prejudice indemnification action, in which harm and causation must be proven.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Chile which affect privacy?

No

11.2 Are there any hot topics or laws on the horizon that companies need to know?

A new Privacy Bill, modelled largely on the GDPR, is being discussed in the Chilean Congress. If approved, the national data protection regime will be completely changed, particularly in terms of enforcement, with the Council of Transparency acting as the data protection authority. In addition, the scale of fines will raise significantly to reach almost $1 million in most extreme cases.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Chile?

The current DPL is clearly below the standard of other more advanced pieces of legislations, such as the GDPR. However, the biggest challenges in implementing foreign privacy policies in Chile are related to having to rely on individual consent, rather than other legal bases of processing available in other jurisdictions, such as legitimate interests. Furthermore, the current law still requires explicit and written consent, which is unusual in more advanced legislations.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The advancement of the Data Protection Bill has moved local companies to anticipate the final approval of the new legislation and define clear privacy programs within their organizations.

12.2 What do you envision the privacy landscape will look like in 5 years?

Considering the influence of the GDPR on various privacy bills, including that in Chile, we envision a normative confluence towards a similar standard to that of the European regulation, in which decision made by the respective European authorities will mark the normative and administrative decisions that are also made in our country. In addition, further sectorial regulations, particularly to finance/banking, critical infrastructure and consumer relations is likely to take place.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The first challenge that most local companies face is that of assessing the amount of personal data that they use and have available within their organizations. This is particularly true in cases where technology has made it increasingly easy to identify individuals through the collection of data, which until a few years ago was insufficient by itself to make an individual identifiable, but now combined with additional information can determine specific characteristics of a person.

CHINA

1 PRIVACY LAW

1.1 How is privacy regulated in China?

There is no specific "Privacy Law" in the People's Republic of China ("PRC"). Rather, China's regulatory framework for privacy protection includes laws and regulations in the civil, criminal and administrative areas, and is gradually evolving. It includes:

(a) the Constitution and the General Principles of the Civil Law: while these do not specifically address "privacy", they do indirectly provide a basis to protect certain rights related to privacy;

(b) the Tort Liability Law: this expressly includes a "right of privacy", and provides that if an individual's privacy is infringed, the individual may bring a civil lawsuit against the injuring party to seek redress. Under the Criminal Law, sale of personal information or illegal acquisition or provision of personal information may constitute a criminal offence;

(c) Decision on Strengthening the Protection of Online Information ("NPC Decision"): In 2012, the Standing Committee of the National People's Congress ("NPC") issued the NPC Decision, which requires enterprises and, in particular, internet service providers to protect the personal electronic information of Chinese citizens. Following the NPC Decision, a sector-specific legal regime in respect of personal information has gradually formed in China, with various departments of the State Council, such as the Ministry of Industry and Information Technology of the PRC ("MIIT"), the State Administration for Industry and Commerce ("SAIC", now merged into the State Administration for Market Regulation, "SAMR"), the Ministry of Public Security ("MPS") and the People's Bank of China ("PBOC") respectively issuing personal information protection regulations under their own administrative authority over the past few years; and

(d) the Cybersecurity Law ("CSL"): the CSL, issued on November 7, 2016 and effective on June 1, 2017, has further enhanced online and network data protections, and is a milestone for personal information protection and data security in the PRC. Following the CSL, several regulations and standards have been issued by relevant authorities to further implement the general data management and privacy requirements of the CSL.

In all of these laws and standards, "privacy" is not given a consolidated definition, but "personal information" is defined under many industry-specific regulations, and generally refers to any information relating to an individual that alone or in combination with other information, can be used to identify that individual. The above regulations and their implementing rules provide a number of general principles for processing and protecting personal information.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(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. 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 personal information, as addressed further below.

(b) **Criminal Law**: Article 253 of the Criminal Law (as provided in Amendment VII to the Criminal Law) applies 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 personal information obtained in his/her employment and where the circumstances are "serious". It is also applicable if an individual illegally acquires such information by stealing or by any other means and where the circumstances are serious. Legal consequences of such acts include fixed-term imprisonment of up to three years, criminal detention or fines.

In the event that an entity commits either of these crimes, the entity is subject to a fine, and the individual in charge, along with any other individuals directly responsible for the criminal activity, is subject to the punishments listed above. Amendment IX to the Criminal Law, which became effective from November 1, 2015, has amended Article 253, and has broadened the scope of personal information-related offences and increased the potential legal liability.

The Supreme People's Court and the Supreme People's Procuratorate have also promulgated an Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Issues Concerning the Application of Law in Handling Criminal Cases of the Infringement of Citizens' Personal Information and relevant typical cases, effective from June 1, 2017, providing more details as to how Article 253 should be interpreted and implemented.

(c) **Tort liability**: The Tort Liability Law, effective as of July 1, 2010, includes many provisions that specifically or generally relate to the protection of personal data, and, in particular, in Article 2, defines the "civil rights and interests" protected under the Law, specifically listing 18 types of rights, including the right of privacy. This was the first time under PRC law that the right of privacy has been treated as an independent type of civil right, and no longer attached to the right of reputation. Under the Tort Liability Law, the violation of the right of privacy and other personal and property rights and interests is clearly provided as constituting a tort. As such, an injured party can seek redress against the injuring party.

(d) **Personal Information Security Standard**: The Personal Information Security Standard ("2018 Standard"), was issued by the State Administration for Quality Supervision and Inspection and Quarantine (now incorporated into the SAMR) and the China National Standardization Management Committee on December 29, 2017, effective May 1, 2018.

The 2018 Standard is a national recommended (not mandatory) standard, but, as currently the most comprehensive general personal information standard, it is very important and has been widely adopted and referred to, and will influence legislation in the future. The most recent draft to amend the 2018 Standard was issued on October 22, 2019, and it is now open for public opinion. There are also several other standards related to personal information and data security that are undergoing a public comment period.

(e) **Industry-specific regulations and rules**: The NPC Decision (see question 1.1), sets forth a number of important principles for handling personal electronic information. Accordingly, various governmental authorities have issued administrative regulations to set out more

specific requirements in their area — including, eg, the MIIT, the SAIC, the POBC, and National Health Commission ("NHC") — and to provide rules for a number of different types of personal information. For example:

(i) Circular of the People's Bank of China on Protecting Personal Financial Information by Financial Institutions, issued by the PBOC on January 21, 2011, effective May 1, 2011;

(ii) Circular of the People's Bank of China on Further Protecting Customer Personal Financial Information by Financial Institutions, issued by the PBOC and effective on March 27, 2012;

(iii) Several Provisions on Regulating the Market Order of Internet Information Services, promulgated by the MIIT on December 29, 2011 and effective March 15, 2012;

(iv) Order for the Protection of Telecommunication and Internet User Personal Information, promulgated by the MIIT on July 16, 2013;

(v) Provisions on the Management of the Security of Personal Information of Postal and Delivery Service Users, issued by the State Post Bureau and effective on March 26, 2014;

(vi) Implementing Measures for Safeguarding Financial Consumers' Rights and Interests, issued by the PBOC and effective on December 27, 2016;

(vii) Circular of the General Office of the Ministry of Human Resources and Social Security and the General Office of the Ministry of Finance on Further Strengthening the Protection of Personal Information in the Information Disclosure for the Use of Employment Subsidies, issued by the Ministry of Human Resources and Social Security and the Ministry of Finance and effective on May 12, 2017;

(viii) Administrative Measures on National Health and Medical Big Data Standards, Safety and Service (trial), issued by the NHC and effective on July 12, 2018;

(ix) Regulations on the Supervision and Examination of Internet Security, issued by the MPS on September 15, 2018, effective November 1, 2018;

(x) Notice on Special Governance of Illegal Collection and Use of Personal Information via Apps, issued by the Office of the Central Cyberspace Affairs Commission, the MIIT, the MPS and the SAMR on January 23, 2019;

(xi) Implementation Rules on Security Certification for Mobile Internet Applications, issued by the Cyberspace Administration of China (CAC) and the SAMR on March 13, 2019;

(xii) Guidelines for Internet Personal Information Security Protection, issued by the MPS on April 10, 2019; and

(xiii) Regulation on Cyber Protection of Children's Personal Information, issued by the CAC on August 22, 2019, effective October 1, 2019;

(xiv) Notice to Rectify Mobile Apps' Infringement on Users' Interests, issued by the MIIT on October 31, 2019; and

(xv) Measures on Identifying Illegal Collection and Use of Personal Information by Apps, issued by the CAC, MIIT, MPS and SAMR on November 28, 2019.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

In the absence of a unified privacy law, regulation and enforcement of privacy-related issues fall to a variety of authorities across all levels of Chinese government, depending on the nature of the infringement.

For example, a breach of the restrictions and requirements for advertising communications (see question 8 below) could result in an investigation from the SAMR, which could lead to an order for rectification plus a fine of CNY 10,000–30,000.

Other breaches of privacy obligations could lead to litigation by the victim under the Tort Law and other laws. The victim could also make complaints to relevant authorities, which could in turn lead to administrative penalties and even criminal liability, depending on the infraction.

Key authorities for privacy-related matters include:

(a) The CAC: responsible for the planning and coordination of cybersecurity and related matters, including personal information protection, along with other authorities;

(b) The MIIT: responsible for supervision and administration of personal information 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 personal information and other privacy-related infractions;

(d) The SAMR: responsible for implementing the Law on the Protection of the Rights and Interest of Consumers;

(e) The China Consumer Association ("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. For example, in June 2018, the CCA initiated an evaluation of privacy policies and data collection by apps in China, and in November 2018 issued the resulting Assessment Report on Personal Information Collection and Privacy Policies by 100 Apps, which pointed out several typical problems such as excessive collection of personal data, use of unclear privacy policies, etc.

On the critical issue of online personal data collection, coordination among these authorities is common, and enforcement efforts can take many forms. For example, on January 23, 2019, the CAC, MIIT, MPS and SAMR jointly issued a Notice on Special Governance of Illegal Collection and Use of Personal Information via Apps, based on which these authorities authorized the National Information Security Standardization Technical Committee, China Consumers Association, the Internet Society of China and the Cybersecurity Association of China to create a special working group on the collection and use of personal information (the "Special Working Group") in violation of laws and regulations.

That Special Working Group then opened a Wechat official account called "App Personal Information Report" and publicized an email (pip@tc260.org.cn) to receive public reports on illegal use and collection of personal information. In April 2019, presumably following complaints, the Special Working Group sent notices to the operators of more than 30 popular apps requiring rectification of various personal information-related issues. Some apps that did not comply in time were then delisted from app stores or had their business licenses revoked. By the end of September 2019, the Special Working Group claims to have evaluated over 600 popular apps, been in contact with the operators of 200 apps and to have rectified over 800 issues.

In a similar vein, on November 4, 2019, the MIIT launched a special campaign to rectify the infringement of users' rights and interests by apps, focusing on four key elements: illegal collection of user personal information, illegal use of user personal information, unreasonable acquisition of user authorization, and setting up obstacles to account cancellation.

2 SCOPE

2.1 Which companies are subject to privacy law in China?

All companies operating in China are potentially subject to laws relating to privacy and personal information. For example, all companies and their employees are generally subject to the Criminal Law and the Tort Liability Law. 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. Further, any company operating in certain industries, such as finance or health care, may be subject to industry-specific rules.

2.2 Does privacy law in China apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, if a company collects personal information from China, it may be subject to relevant rules relating to data transfers and localization. Some of the relevant laws are still in draft form, but this will be an area of increasing obligations for foreign entities. Please see further question 9.1.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in China?

Under the CSL, "personal information" refers to all kinds of information recorded by electronic or other means that can be used to independently identify or be combined with other information to identify natural persons' personal information, including but not limited to: natural persons' names, dates of birth, ID numbers, biometric information, addresses and telephone numbers, etc.

The 2018 Standard further classifies personal information as basic personal information, personal biometric information, internet identity information, personal physical health information, personal educational and career information, personal financial information, personal communication information, personal contact information, personal location information, etc., and sets out several examples for each of these categories.

For instance, "personal financial information" under the 2018 Standard includes bank account information, identification information (code), deposit information (including the amount of deposits, records of receipts and payments, etc.), real estate information, credit loan records, credit reference information, records of transactions and consumption, flow records, etc., and information about virtual property (such as virtual currency, virtual transactions, and key codes for games). Further, the draft Trial Measures on the Protection of Personal Financial Information and Data circulated by the PBOC on September 10, 2019, define "personal financial information" as including identity information, bank account information, asset information and other financial information.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Under the 2018 Standard, personal information is subdivided into general information and sensitive information. "Sensitive personal information" is personal information that may endanger personal and property safety, easily cause damage to personal reputation, physical and mental health or cause discriminatory treatment if leaked, illegally provided or abused. This includes ID number, personal biometric information, bank account number, communication records and contents, property information, credit information, location information, accommodation information, health and physiological information, transaction information, personal information of children aged 14 and under, etc. Sensitive personal information can only be collected with the user's affirmative consent, which is clear, specific and given on a fully informed basis.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

In addition to certain existing and pending data transfer and localization requirements (see question 9 below), the key principle for personal information handling in the PRC is consent, accompanied by a number of other general and specific principles addressing the security and scope of data collection, and the rights of the data subject. Key rules in this respect are provided in the CSL and the 2018 Standard, as follows:

(a) The CSL outlines three general principles for the handling of personal information:

  (i) Transparency: The CSL requires that network operators shall make public the rules for collecting and using personal data, and expressly notify users of the purpose, methods and scope of such collection and use.

  (ii) Lawful basis for processing: The CSL requires the network operators abide by the principles of "lawful, justifiable and necessary" when collecting and using personal data.

  (iii) Purpose limitation: The CSL requires that network operators not collect any personal data that is not related to the service being provided.

(b) The 2018 Standard identifies a number of other or more enhanced obligations for the handling of personal information, including:

  (i) Consistency of responsibility: ie, personal information controllers should be responsible for damage caused by their personal information processing activities to the legitimate rights and interests of the subject of the personal information;

  (ii) Clarity of purpose: ie, personal information processing should be legitimate, justified, necessary and have clear purposes;

  (iii) Choice and consent: ie, informing the subject of the personal information of the purpose, mode, scope and rules for personal information processing and seeking authorization and consent;

  (iv) Minimum sufficiency: ie, except as otherwise agreed by the subject of the personal information, only the minimum type and quantity of personal information needed to satisfy the purpose should be collected, and when the purpose is achieved, the personal information should be deleted in time according to the agreement;

(v) Openness and transparency: ie, the scope, purpose and rules for dealing with personal information should be publicized in a clear, understandable and reasonable way, and be subject to external supervision;

(vi) Security: ie, network operators should have security capabilities matching the security risks of the personal information collection, and sufficient management measures and technical means should be adopted to protect the confidentiality, integrity and usability of the personal information; and

(vii) Subject participation: ie, providing for access, correction and deletion of personal information and a method to withdraw consent or cancel an account for the subject of the personal information.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Chinese law does not generally distinguish between data collectors, data controllers, data processors, etc, but some newer rules are beginning to make such distinctions. For example, the 2018 Standard introduces certain obligations that "data processors" should comply with during any data "entrusted processing", ie, where a data controller entrusts another party to process personal data on the controller's behalf. In such case, the controller should enter into an agreement or use other formalities to address the responsibilities and duties of the processor.

In the context of personal information collection, the key regulated categories are network operators, which include nearly all companies with a material online presence, and CII operators, which are subject to stricter requirements in respect of data security, eg:

(a) to set up independent security management institutions and designate persons responsible for security management, and review the security background of the said responsible persons and personnel in key positions;

(b) to periodically conduct cyber security education, technical training and skill assessment for practitioners;

(c) to make disaster recovery backups of important systems and databases; and

(d) to formulate contingency plans for cyber security incidents, and carry out manoeuvres periodically etc.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

In brief, the key obligations include the following:

(a) complying with the principles of lawfulness, fairness and necessity and other key privacy principles listed above when collecting and using personal information;

(b) informing data subjects explicitly of the purpose, methods, and scope of the collection and use of the personal information, and obtaining their consent;

(c) publishing statements describing the collection and use of personal information;

(d) keeping personal information strictly confidential, and refraining from disclosing, selling or illegally providing such information to others without consent;

(e) taking necessary measures to ensure the security of personal information and, in the event of the disclosure or loss of such information, immediately taking remedial measures; and

(f) refraining from sending any commercial messages to an individual without his or her consent or request, or if the individuals has expressly refused to receive such information.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in China? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

(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, for establishing and improving their systems for user information protection, and for preventing such information from being divulged, damaged or lost. The 2018 Standard also provides that, if the network operator appoints a third party to process personal data on its behalf, it shall ensure that such processor will provide an adequate level of protection to the personal data involved.

(b) On June 27, 2018, the MPS released for public comment a draft of the Regulations on Cybersecurity Multi-level Protection Scheme (the "Draft MLPS Regulation"). The Draft MLPS Regulation updates the existing MLPS, a framework dating back to 2007. Both the original and the updated Draft MLPS Regulation uses a one-to-five scale to classify information systems physically located in China, based on their relative potential impact on national security, social order, and economic interests, with one being the least critical and five being the most critical. Network operators that are classified (initially self-assessed and proposed by operators, and then confirmed by MPS) at level 3 or above are subject to enhanced security requirements. The updated Draft MLPS adjusts the classification criteria for levels 2 and 3, and provides more obligations for operators classified at level 2, and those at level 3 or above.

(c) In September 2018, the MPS issued Regulations on the Supervision and Examination of Internet Security. These regulations authorise the police to inspect the network security of providers of the following services:

(i) internet connection services, internet data centres, content delivery networks and domain services;

(ii) internet information services;

(iii) internet cafe services; and

(iv) other internet services (not defined, but could cover nearly all services constituting the internet industry in China).

These regulations summarise and consolidate the security obligations of internet service providers set out in the Cybersecurity Law and a series of regulations and circulars applicable to different types of internet service providers. These regulations generally give the police authority to conduct on-site inspection of an internet service provider's place of business and carry out remote testing of network loopholes. The powers of the police and the procedures for inspecting internet service providers and imposing penalties are still being clarified.

(d) During the year 2018-2019, the National Information Security Standardization Technical Committee formulated and announced a series of national recommended standards under which information security technologies are to be regulated.

6.2 How are data breaches regulated in China? What are the requirements for responding to data breaches?

There is no specific definition of "data breach" in either the CSL or the 2018 Standard. However, under the CSL, in case of possible disclosure, damage or loss of data, the network operator is required to take immediate remedies and report the issue to the competent authority. The 2018 Standard provides that the report should include the type, quantity, content and nature of the affected data subjects, the impact of the breach, measures taken or to be taken, and the contact information of relevant persons at the company.

The Administrative Measures for Data Security (draft for comments) issued by CAC on May 28, 2019 provides that a network operator must, in the case of any data security incident involving personal information disclosure, damage, loss, etc., or any significantly increased risk of the occurrence of a data security incident, immediately take remedial measures and promptly notify the relevant personal information owner by phone, SMS, mail or letter, and inform the competent supervisory authority in charge of the industry and competent cyberspace administration as required. If a network operator violates these provisions, it may, in light of the circumstances, be penalized by public notice, confiscation of illegal gains, suspension of related business, cessation of business for rectification, closure of website, or revocation of the relevant business permit or business license by the competent authority. If the acts rise to the level of a crime, then criminal liability is also possible.

Under the Criminal Law, "network service providers" who do not fulfil legal obligations regarding information network security management, refuse to make corrections after being ordered by the relevant authorities, and therefore causing leakage of users information with serious consequences, may face a sentence of imprisonment or criminal detention of not more than three years or surveillance, with a fine or a fine only.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Under the CSL and the 2018 Standard, individuals have the following key rights in relation to the processing of their personal information:

(a) right of access to data, copies of data;

(b) right to rectification of errors;

(c) right to deletion/right to be forgotten;

(d) right to object to processing;

(e) right to restrict processing;

(f) right to data portability;

(g) right to withdraw consent;

(h) right to object to marketing; and

(i) right to complain to the relevant data protection authorities.

Some of these rights are relatively new or not clearly defined, and there is some inconsistency in market practice.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Generally, the NPC Decision provides that no organization or individual may send commercial electronic messages to fixed line or mobile telephones or the email of an individual without the prior consent or request of the recipient or if the recipient explicitly express his/her refusal.

In addition, under Article 43 of the Advertisement Law, no advertisements may be distributed via electronic means without obtaining the recipient's consent. Advertisements distributed via electronic means must state the true identity and contact details of the sender, and a method for the recipient to refuse acceptance of future advertisements.

The Administration of Internet Electronic Mail Services Procedures provides that if an email recipient who has expressly consented to receive electronic direct marketing subsequently refuses to continue receiving such email, the sender must stop sending such emails unless otherwise agreed by the parties.

Further, under the 2018 Standard, the consent of relevant data subject much be obtained for advertising in electronic or other forms using personal data. If the data subject revokes his/her consent for data processing, the data controller may not continue sending such advertisements.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is no legislation explicitly addressing the use of tracking technologies. But as many of these tracking methods fall within the definition of personal information in accordance with the 2018 Standard, it is understood that general regulations on personal data apply to the use of tracking technologies.

The 2018 Standard also 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 personal information, and how the user can restrict Cookies or other similar technologies from collecting personal information.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The Guidelines for Internet Personal Information Security Protection provide that user profiling technology, which relies entirely on automated processing, can be applied to value-added applications such as precision marketing, search results ranking, personalized push news, targeted advertising, etc without explicit user authorization in advance, but that users should be guaranteed the right to object or refuse. If applied to value-added applications that may bring legal consequences to users, such as credit information services, administrative and judicial decision-making, or used by cross-network operators, such data processing should be explicitly authorized by users.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Explicit consent from the data subject is required for sharing data with a third party. The source of the data must also have been collected legitimately and lawfully. It is relatively easy to track this through user terms for data collected online, but is more challenging for data collected offline.

8.5 Are there specific privacy rules governing data brokers?

Currently, there are no specific privacy rules in this regard. As data brokers fall within the scope of network operators under the CSL and its many related regulations, the general rules will apply, especially as to user consent, scope of collection, and similar data management rules and rights. Moreover, more rules are becoming applicable to these kinds of data crawls and brokered sales over time. For example, the Administrative Measures for Data Security (draft for comments) sets more details and limits for network operators which collect data and crawl the internet for user information. In particular, where the network operator accesses and collects data of a website by automated means, it may not hinder the normal operation of the website. If such automated access and collection seriously affect the operation of the website, eg, if the traffic from that exceeds one-third of the website's daily average traffic, it must be stopped, upon the website's request. In addition, it should be noted that authorities are strengthening their supervision of data brokers who illegally collect personal information. In September 2019, several data companies located in Hangzhou and Shanghai were investigated by the local authorities and had to suspend their data broker services. These companies illegally collected personal information including credit information, shopping records, social media records and even fees paid for telecoms, gas or electricity, and provided such integrated information to online lending platforms.

8.6 How is social media regulated from a privacy perspective?

There are no specific privacy rules in this regard. As social media operators also fall within the scope of network operators, and sometimes even CII operators, the general rules for those categories of data processors will apply.

In addition, there are several requirements and limitations on the collection of personal information through apps including social media apps, including the Guidelines on Self-evaluation of Illegal Collection and Use of Personal Information by Apps issued in March 2019, and the Measures on Identifying Illegal Collection and Use of Personal Information by Apps (Draft for comments) issued in May 2019.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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 user personal information, then it will have to comply with the general rules for the protection of personal information.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

(a) The CSL provides that the personal information and important data collected by a CII operator during operations within the territory of PRC must be stored domestically. Cross-border transfer is only allowed if necessary to satisfy business needs, and will in any event be subject to the completion of a security assessment and approval from the competent industry authorities. As mentioned in question 1.2, a CII operator is an entity who operates information infrastructure used for public communications and information service, 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, national economy or the public interests if destroyed, damages or suffering a data leakage.

(b) The Draft Measures on the Security Assessment of Personal Data and Important Data to be Transferred Abroad (Draft for Comment) issued by the CAC on April 11, 2017 were intended to provide more details on these obligations. Crucially, this draft expanded the data localization requirement to all network operators, which caused a significant reaction among industry stakeholders.

The 2017 draft was updated with a new draft in 2019 titled as the Draft Measures on the Security Assessment of Personal Data to be Transferred Abroad (Draft for Comment), which removes the explicit data localization requirement for network operators, and instead focuses on the requirement to fulfil a "security assessment" before any cross-border transfer of personal information. The 2019 draft also clearly specifies that "foreign entities" will be required to fulfil the relevant obligations under the 2019 draft through their authorized representatives or affiliates in China if they collect the personal information of Chinese users through the internet.

The specific procedures for these proposed "security assessments" are not detailed in these drafts, and nor is there any specified mechanism for foreign entities to comply with these proposed rules if they do not have a local entity. These details and many others will presumably be addressed in future drafts or implementing rules.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

The principles outlined above generally apply to all data transfers.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Under the CSL, for a "severe" violation, an operator or provider may face fines of up to RMB 1 million (or 10 times 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.

Data security breaches may also involve criminal liabilities. Article 286(A) of the Criminal Law stipulates that network service providers who 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 by the relevant authorities (therefore causing the leakage of user's information with serious consequences), may face a sentence of imprisonment or criminal detention of not more than three years or surveillance, with a fine, or a fine only.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes, individuals can sue for civil compensation if their privacy rights or reputation are harmed. Such lawsuits would generally be brought under the Tort Liability Law or the Law on the Protection of the Rights and Interest of Consumers.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of China which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Data localization and illegal or harmful data handling by companies are priority topics for both the public and the regulators in China right now, and the laws reflect this. Following the promulgation of the CSL, there have been numerous new standards, measures and other rules issued by the authorities designed to clarify the requirements for companies and individuals. However, many of these new rules remain in draft form, and there has sometimes been significant variation between versions of these drafts, so there is still considerable uncertainty as to what the final data handling and data transfer regime in China will look like. Nevertheless, there is a strong trend towards data localization, which is of particular concern to foreign companies operating in or advertising and collecting data in China.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in China?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

China legislators are gradually releasing more laws focussing on cybersecurity, network security, including personal information protection, along with the strengthening enforcement. Many relevant regulations targeting this were issued in 2019, in final or draft form, including the Administrative Measures for Data Security, the Personal Financial Information and Data Protection Measures and the Personal Information Security Standard, and some are already issued and in effect, such as the Implementation Rules on Security Certification for Mobile Internet Applications, the Guidelines for Internet Personal Information Security Protection, and the Regulation on Cyber Protection of Children's Personal Information. This is part of a wider trend towards better regulation and protection of what is called cybersecurity sovereignty, which we expect will create more and more onerous

requirements for companies across the spectrum of scale, industry, and national origin. This also tracks and is enabled by a growing global scepticism of corporate data handling in general, as exemplified by the GDPR and related rules.

12.2 What do you envision the privacy landscape will look like in 5 years?

The CSL and its many related rules have many provisions that are still very general and abstract. The next five years will see these rules clarified, and the true extent of regulation will be revealed by enforcement actions. It is very difficult to anticipate exact outcomes, as the PRC 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 tighter regulation and enforcement of data and privacy issues will be the strong trend.

12.3 What are some of the 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 the fact that many of the relevant rules remain in draft form. This means that companies need to be flexible and need to prioritize staying up-to-date on the continuously evolving requirements and expectations.

COLOMBIA

1 PRIVACY LAW

1.1 How is privacy 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The key regulations concerning privacy are the following:

(a) Law 1266 of 2008: by which the general provisions of *habeas data* are established, and the management of the information contained in personal databases, especially databases with financial, credit, commercial or services related content and those from third countries is regulated.

(b) Decree 1727 of 2009: which sets out the way in which the operators of financial, credit, commercial and services databanks, and those from third countries, must present the information of data subjects.

(c) Law 1581 of 2012 ("Data Protection Statute"): by which general provisions for the protection of personal data are issued.

(d) Decree 1377 of 2013: by which the Data Protection Statute is partially regulated, in order to facilitate its implementation and compliance. In particular, aspects related to:

  (i) the authorization of the data subject for the treatment of his/her personal data,

  (ii) the policies relating to data processing and the data controller,

  (iii) the exercise of the rights of data subjects,

  (iv) transfers of personal data, and

  (v) responsibility towards the processing of personal data.

(e) Law 1712 of 2014: through which the law of transparency and the right of access to national public information is created.

(f) Decree 886 of 2014: which regulates the National Registry of Databases.

(g) Law 1928 of 2018: through which the "Convention on Cybercrime" is adopted.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Privacy law can be enforced as follows:

(a) **Direct claims**: A data subject or its successors 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**: The data subject or its successors may only file a complaint with the Superintendence of Industry and Commerce ("SIC", the competent authority) 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 SCOPE

2.1 Which companies are 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: 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: 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The Data Protection Statute applies to the processing of personal data carried out in the Colombian territory or 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 INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" is all information that may affect the privacy of the data subject or whose improper use may generate discrimination, such as those 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 he/she is physically or legally incapacitated. In these events, legal representatives must grant their 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 syndicates, provided that they relate exclusively to its members or to persons who have regular contact because of their purpose. In these events, 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.

(e) The processing has a historical, statistical or scientific purpose. In this event, the measures leading to the removal of identity of the data subjects must be adopted.

The processing must ensure respect for the prevailing rights of children and adolescents (The processing of 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

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 him/her 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.

(g) **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.

(h) **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, being able only 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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

There are two main roles that may concur in one person/entity:

(a) **Data Controller**, who is in charge of the collection of the information. Thus, the data controller is required to obtain authorization from the data subject concerning the processing of the personal data.

(b) 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

(a) The obligations shared by the data controller and the data processor are the following:

(i) to guarantee to the data subject, at all times, the full and effective exercise of the right of *habeas data*;

(ii) to keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access;

(iii) to update the information and take the other necessary measures so that the information provided to it is kept updated;

(iv) to process any queries and claims made in accordance with the Data Protection Statute;

(v) to adopt an internal manual of policies and procedures to ensure proper compliance with the Data Protection Statute, especially regarding inquiries and complaints; and

(vi) to comply with the instructions and requirements issued by the SIC.

(b) The obligations of the data controller are the following:

(i) to request and keep, under the conditions required in the Data Protection Statute, a copy of the respective authorization granted by the data subject. This authorization may be required by the authority in case there is a complaint from the data subject;

(ii) to duly inform the data subject about the purpose of the collection of the information and the rights that assist him/her by virtue of the authorization granted. All advertising purposes must be included and accepted by the data subject in order to be able to send advertising to the contact information provided by the data subject;

(iii) to ensure that the information provided to the data processor is true, complete, accurate, updated, verifiable and understandable;

(iv) to rectify the information when it is incorrect and communicate the pertinent to the data processor;

(v) to provide the data processor, as appropriate, only data whose processing is previously authorized in accordance with the provisions of the Data Protection Statute;

(vi) to require the data processor, at all times, to have respect for the security and privacy conditions of the data subject's information;

(vii) to inform the data processor when the data subject has submitted a claim concerning his/her personal information and the respective procedure has not been completed;

(viii) to inform the data subject, at his/her request, about the use given to his/her personal data; and

(ix) to inform the SIC when there are violations of security codes and risks in the administration of the information of the data subjects.

(c) The obligations of the data processor are the following:

(i) to timely update, rectify or delete the data in the terms of the Data Protection Statute;

(ii) to record in the database the legend "claim in process" in the way it is regulated in the Data Protection Statute;

(iii) to insert in the database the legend "information in judicial discussion" once notified by the competent authority about judicial processes related to the personal data;

(iv) to refrain from circulating information that is being disputed by the data subject and use of which has been suspended by the SIC;

(v) to allow access to information only to those who may have access to it; and

(vi) to inform the SIC when there are violations of security codes and there are risks in the administration of the information of the data subjects.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Colombia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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.

6.2 How are data breaches regulated in Colombia? What are the requirements for responding to data breaches?

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 (For example, in a case against a Bank in Colombia, the SIC pointed out that the Bank 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.

(c) All the measures taken to undermine the breach and its effects (In the same case against the Bank, the SIC found that the Bank had failed to prove the security protocols to limit or minimize the risks for the processing of personal data).

(d) 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 would 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."

Hence, 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, based on security breach, the penalty was reduced from 40 to 30 times the monthly legal minimum wage (approximately US $8,280), since the University accepted that it had suffered a security breach.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

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, among others, against partial, inaccurate, incomplete, fractional, error-inducing data, or those 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 his/her personal data.

(d) To submit complaints to the SIC for violations of the provisions of the Data Protection Statute and the other related regulations.

(e) To revoke the authorization and/or request the deletion of the 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 incurred in conduct contrary to the Data Protection Statute and/or the Constitution.

(f) To access free of charge to the his/her personal data that has been subject to processing.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The only contact information which can be used to send marketing communications is that which the data subject has explicitly authorized use of. 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 a proceeding against the advertiser.

This has been studied in several decisions from the SIC, in which it is clear that the gathering of the contact information must be previously authorized (or the latest at the moment of collection) and that the use for which the information is being collected should be clear and sufficient so the data subject can control the use of his/her information.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

This is governed by the general principles explained in question 3.3.

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 its 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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertising and behavioral advertising are 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. This translates into a proscription on being subjected to adverse legal effects due to an evaluation of their personality through an automated treatment of data intended to evaluate certain aspects of their personality, or in connection with data that is considered as sensitive.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

As the privacy right is based upon self-determination and freedom, the notice of consent collected should be clear and sufficient so the data subject can control the use of his/her information.

The uses and the scope of such uses which are to be given to their personal information should be made clear to the data subject.

8.5 Are there specific privacy rules governing data brokers?

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 which the operator who delivers the data has; and

(i) the persons authorized by the aforementioned law.

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.

8.6 How is social media regulated from a privacy perspective?

(a) **Social Networks**: These cannot collect or treat personal information without free, prior and express consent from the data subject.

(b) **Third Parties**: The data controller may only contact the data subject through the mechanisms previously and expressly authorized by him/her, 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 disclosed information that may affect the privacy of others or affect their image or good standing.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs are authorization-based. Thus, programs can only use information for the purposes expressly permitted by the data subject.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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 shall not apply :

(a) where the data subject has granted his/her 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.

(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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Companies interested in international data transfer are required to obtain a declaration of conformity from the SIC.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 (US $480,000 approx). 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.

(d) Immediate and definitive closure of an operation that involves the processing of sensitive data.

10.2 Do individuals have a private right of action? What are the potential remedies?

Individuals have a private right of action; however, the proceeding does not contemplate compensation for damages for the data subject and remedies would be the those described in question 10.1, that is, fines, suspension or closure.

If there is a damage that should be compensated, the individual should initiate a declarative civil proceeding.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Colombia which affect privacy?

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 Are there any hot topics or laws on the horizon that companies need to know?

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 cautions around processing personal information/personal data in Colombia?

The main caution in Colombia is the importance to safeguard the authorization granted by the data subject, as proof of his/her consent might be required by the competent authority.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The importance of privacy in a time where boundaries have been getting more and more blurred. However, the changes have been extreme as companies have had to adapt and modify conduct which had been the norm for all their lives.

12.2 What do you envision the privacy landscape will look like in 5 years?

Recognition of data subjects and the value of the data they provide. Payment to individuals for the provision of private data.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

One of the main consequences of the Data Protection Statute has been that companies have had to modify the way they contact their clients and how they obtain new clients.

COSTA RICA

1 PRIVACY LAW

1.1 How is privacy regulated in Costa Rica?

Data protection in Costa Rica is regulated by the Law for the Protection of Individuals Regarding the Processing of their Personal Data No 8968 of 2011 ("Data Protection Law") and Regulation of the Executive Law on the Protection of Persons Regarding the Processing of their Personal Data (Decree No 37554-JP) ("Data Protection Regulation").

However, the right to data protection was recognized and protected in Costa Rica before the enactment of the Data Protection Law, through several decisions issued by the Constitutional Court from the 1990s onwards. This right was understood to be derived from Article 24 of the Political Constitution of Costa Rica, which protects the right to intimacy, as well as the freedom and secrecy of communications.

The main regulator in Costa Rica is the Agency for the Protection of Inhabitants' Data ("PRODHAB") and PRODHAB's main duties and responsibilities, among others, are:

(a) Processing any claim related to a data protection matter;

(b) Administrating the registration procedure of those databases that must comply with such requirement;

(c) Requesting any information regarding the data processing made by any entity;

(d) Creating awareness and promote the protection of personal data;

(e) Elaborating guidelines for any aspect regarding data protection; and

(f) If needed, issuing mandatory orders to data controllers to ensure compliance with the data subjects' rights.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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 the Regulation of the Consumer Protection Law (Decree No 37899-MEIC) ("Consumer Protection Regulation").

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The regulator in Costa Rica is PRODHAB. However, the National Consumer's Commission ("CNC") also has jurisdiction when consumer protection issues are involved (mainly in the context of e-commerce transactions). There is no self-regulatory body dealing with privacy.

2 SCOPE

2.1 Which companies are subject to privacy law in Costa Rica?

Any company (private or public) that processes personal data contained in automated databases or manuals is subject to the privacy law in Costa Rica, regardless of its location.

2.2 Does privacy law in Costa Rica apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The Data Protection Law is applicable to anyone storing or using data of a Costa Rican resident. It is also applicable when so stated in a contract or by any rule of international law. Foreign based entities are not required to have a local representative (unless the database must be registered, in which case appointing a representative is a duty of both local and international entities), but their actions will be subject to Costa Rican laws.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Costa Rica?

Article 3 of 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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.

(c) Sensitive Personal Data: information concerning the intimate realm of the person, that may not be stored except in very specific circumstances. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, spiritual convictions, socioeconomic condition, biomedical or genetic information, health, sexual life and orientation.

Data subjects have the right to refuse to provide sensitive data, and, when such data is provided, it may not be processed without the express consent of the data subject. The exceptions are where:

(i) the processing 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) the processing 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) the processing relates to sensitive personal data that the data subject has voluntarily made public, or is required for the recognition, exercise or defence of a right in judicial proceedings; or

(iv) the processing 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

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.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

There are no relevant provisions for agreements between data controllers and data processors. The only aspect related to this matter is provided in Article 30 of 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 also 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Before making outbound calls for marketing/sales purposes, entities must obtain prior consent from the recipient in order to process his personal information. The consent must be express, unequivocal and informed, so that the data subject has been given the following information:

(a) the existence of the database,

(b) use that will be given to the information,

(c) who will be the recipients of the information,

(d) whether or not it is mandatory to provide the information,

(e) consequences for not providing the information,

(f) how the information will be safeguarded,

(g) mechanisms allowing individuals to consult, amend, update, and suppress personal information; and

(h) authorization for transferring the database to a third party.

As exceptions to this rule, cold calling is allowed when:

- the client has previously expressed its willingness to receive any of the communications otherwise covered by the prohibition; or
- in the context of a previous sale or commercial relationship, that same supplier uses the information provided by the client to promote the sale of similar products or services and/or pretends to solve any issue with the transaction.

Additionally, any marketing communication made by email, SMS or phone must clearly identify the sender. It must also be done simply enough to easily identify the purpose of the message. All messages must 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Costa Rica? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

There are general obligations of confidentiality and security for the processing of personal information:

(a) The security obligation is included in the Data Protection Law, which 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 the personal data.

(b) The duty of confidentiality provides that the data controller and those involved in any phase of the processing of personal data are bound by professional or functional secrecy, even after

the end of their relationship with the database. A person may be relieved of the duty of secrecy by a court decision where strictly necessary.

6.2 How are data breaches regulated in Costa Rica? What are the requirements for responding to data breaches?

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 term (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) nature of the incident;

(ii) compromised data;

(iii) corrective measures immediately taken upon notice of the breach; and

(iv) contact information and place where more details about this matter can be obtained.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Data subjects have the right, when requested to provide their personal information, to an informed consent (see question 5.1). Express consent is not needed in the case of a few exceptions, namely:

- 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;
- it is personal data of unrestricted access, obtained from sources of general public access; or
- the data must be provided as a result of a constitutional or legal provision.

The main rights of each data subject are:

(a) **Right of access**: 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;

(b) **Right of rectification**: data subjects are entitled to request the modification of all incomplete, inaccurate, and/or unclear data; and

(c) **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 anonymised.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Initially, marketing communications were regulated in the Telecommunications Law, which covered only direct sales. However, subsequent regulations have extended this rule to cover also other forms of commercial communications, such as promotional marketing and/or advertising in general. Any marketing communication made through email must clearly identify the sender. It must also be done simply enough to easily identify the purpose of the message. Additionally, all messages must 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 (the definition mentioned below is the one contained in the regulation):

(a) Unsolicited advertising ("adware"): Information sent through the web to users related to the sale of a product or a service without the consent of the recipient.

(b) Unsolicited communications: 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.

(c) Unauthorized operation of, access to and monitoring a terminal: 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.

(d) Spreading viruses: Sending mass emails or other messages with the purpose or the consequence of contaminating the recipient terminal with a virus.

(e) Unsolicited mass emails (SPAM): Emails of unknown senders within the web, who constantly change their domains or usernames with the purpose of defeating the filters against unwanted messages.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is no specific regulation for using tracking technologies.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There is no specific regulation for targeted and behavioral advertising. Thus, the general regulations regarding data protection and informed consent will apply.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The Data Protection Law requires that data controllers obtain consent from the data subject in order to transfer personal data to another country (It does not include special regulations for specific countries. All countries have the same requirements.) Also, the transferor must ensure that, where information is transferred to any other country, adequate levels of protection of the data subject's rights in connection with the processing of their personal data will be provided.

8.5 Are there specific privacy rules governing data brokers?

No, there is no specific regulation for data brokers.

8.6 How is social media regulated from a privacy perspective?

There is no specific regulation for social media from a privacy perspective.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs are regulated by general data protection regulations.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See question 8.4.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

When personal data is transferred to a data processor for processing purposes only (ie, the processor does not become a data controller), or is moved between companies of the same economic group, or to companies under joint control, the transfer of data to the data processor does not constitute a transfer under the Data Protection Law, and it is not necessary to obtain the data subject's consent.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The competent authority in charge of imposing sanctions against non-compliance of 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 being discussed, the case would be decided by the Constitutional Court, or, in the context of an e-commerce transaction, the CNC 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, and fines can range from approximately $3,000 to $18,000.

10.2 Do individuals have a private right of action? What are the potential remedies?

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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Costa Rica which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

No, there are no hot topics or laws at this time.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Costa Rica?

No, everything has been covered.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

There haven't been any important change in the past few years.

12.2 What do you envision the privacy landscape will look like in 5 years?

At this time, we do not foresee any important modification in the privacy landscape in Costa Rica.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

One of the main challenges in Costa Rica is the lack of culture from the individuals and the managers in general.

CURACAO

1 PRIVACY LAW

1.1 How is privacy regulated in Curacao?

Privacy law in Curacao is based on the Privacy Ordinance (Official Gazette 2010 no 84).

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Privacy law is based on the Privacy Ordinance (Official Gazette 2010 no 84).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The Commission for Protection of Personal Data is in charge of supervising compliance with the Privacy Ordinance and administrative enforcement; however, the members of this Commission have yet to be appointed. Infringers can also be prosecuted via civil and criminal actions.

2 SCOPE

2.1 Which companies are subject to privacy law in Curacao?

Companies subject to privacy law in Curacao are those legal entities established in Curacao that process personal data in connection with activities in Curacao.

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 Curacao apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Privacy law applies to companies outside Curacao if they are using automated or non-automated means located in Curacao, unless these means are only used for the transfer of personal data. Companies outside Curacao may only process personal data if a resident representative is appointed.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Curacao?

"Personal information" is any information concerning an identified or identifiable natural person.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The term "sensitive personal data" is not used in the Privacy Ordinance. The Privacy Ordinance maintains the term "exceptional personal 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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

(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.

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.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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 thereof and supervises compliance by the processor with such measures. In addition, the controller ensures that the processor processes personal data further to his 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 Curacao, 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

There are no specific advertising privacy requirements. 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 DATA SECURITY AND BREACH

6.1 How is data security regulated in Curacao? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

There must be appropriate technical and organizational measures to secure personal data against loss or wrongful processing. The Curacao Bureau for Telecommunication and Post has issued guidelines in this regard. Also, recommendations pertaining to the GDPR can serve as a guideline.

6.2 How are data breaches regulated in Curacao? What are the requirements for responding to data breaches?

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 under penalty of the Commission for Protection of Personal Data rectifying the violation itself, or under penalty of the payment of a fine if the order is not complied with in a timely or proper fashion. Individuals may also pursue civil or criminal enforcement.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals have a right to be informed if their personal data is being processed, they must 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 can request that their personal data be modified, protected or deleted.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

There are no specific stipulations for such notice or consent. 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. For example, clear written consent from the individual for use of personal data and sharing thereof with third parties, and clear notification to the individual regarding what kind of personal data is collected and used and for what purpose, and of appropriate measures taken to protect the personal data.

8.5 Are there specific privacy rules governing data brokers?

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.

8.6 How is social media regulated from a privacy perspective?

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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

There are no requirements or restrictions concerning data transfer to a country that belongs to the Kingdom of the Netherlands (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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

It is advisable for individuals to be made aware about matters such as the kind of personal data that will be transferred, to what party, where it will be stored, and the type of protection that is offered thereto.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Potential penalties or sanctions for violations of privacy or data security law are:

(a) administrative sanctions, such as the issuance of an order under administrative enforcement or a penalty;

(b) criminal sanctions such as a penalty up to max ANG 10,000 or a prison sentence; and

(c) civil sanctions such as damages.

10.2 Do individuals have a private right of action? What are the potential remedies?

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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Curacao which affect privacy?

Curacao is a relatively small community, so this urges controllers and processors to observe extra due care in processing personal data.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

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.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Curacao?

Considering that the Privacy Ordinance is based on the Dutch Privacy Act (the Dutch Privacy Act has, in the meantime, 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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

There have been no changes to the Privacy Ordinance, other than a profile sketch for persons to be appointed to the Commission for Protection of Personal Data. The members have not been appointed as yet.

12.2 What do you envision the privacy landscape will look like in 5 years?

Hopefully, the members to the Commission for Protection of Personal Data will be appointed by then and the Commission will be active.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Practical information on the implementation of measures to protect personal information.

DOMINICAN REPUBLIC

1 PRIVACY LAW

1.1 How is privacy regulated in the Dominican Republic?

Privacy is a fundamental right included in Article 44 of the Dominican Republic Constitution, which says: "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 that statement, the Article refers as consequences:

(a) the inviolability of the home;

(b) the right to data protection; and

(c) the inviolability of the secrecy of telecommunications.

Beyond the Constitution, the Dominican courts have taken into consideration international treaties such as the Universal Declaration of Human Rights and the International Pact of Civil and Political Rights.

There are also special data protection and anti-spam laws, that specifically concern privacy.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The Dominican Republic has the following laws concerning specific areas:

(a) General: Data Protection Law No 172-13;

(b) Advertising: Anti-Spam Law No 31-14;

(c) Privacy of telecommunications by any means is also regulated by several Laws, such as:

  (i) Telecommunications Law,

  (ii) Technology Crimes Law No 53-07,

  (iii) Criminal Procedure Code, and

  (iv) Ecommerce is also regulated by several resolutions from the Telecommunications Agency;

(d) Law on the Protection of the Image, Honor and Family Intimacy Linked to Deceased and Injured Persons, the main objective of which is to prevent the publication, in any sort of media, pictures of injured or deceased individuals in accidents. Social media, TV and press are included in this legislation; and

(e) There is also an autoregulatory code, that it is not being enforced, that includes principles and rules on respect of privacy and intimacy of the persons.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

There is no data protection authority in the Dominican Republic. Rather, privacy is enforced by courts in civil and constitutional matters.

The District Attorney and the police enforce the legislation when a crime is committed, eg, when there is illegal interception tapping, spying on data transmission or telecommunications or there an illegal access to a database. The District Attorney also has jurisdiction if there is "any violation" of the Data Protection Law, and also if a person consults without permission databases of credit bureaus.

On the other hand, the Banking Superintendence, which is an institution formed for the inspection and control of the operations of banking institutions in the Dominican Republic, has authority as control agency to inspect the personal data processing of information or credit bureaus. However, credit bureaus do not have an obligation to register databases or to notify the transfers.

The Dominican Commission of Advertising Autoregulation ("CODAP") has been created, but has not been implemented.

2 SCOPE

2.1 Which companies are subject to privacy law in Dominican Republic?

Generally speaking, all persons and companies are subject to privacy legislation in the Dominican Republic.

In addition, credit bureaus have to comply with detailed and specific rules laid out in the Data Protection Law.

2.2 Does privacy law in Dominican Republic apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Dominican data protection rules do not apply outside the country.

As regards privacy matters, where an illicit action or crime is committed with effects in the Dominican Republic, and the entity that originates or orders the illicit action is outside the Dominican Republic, Dominican Law and Courts are competent for enforcement against such action.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Dominican Republic?

The Data Protection Law defines "personal information" as: "Any numerical, alphabetical, graphic, photographic, acoustic or other information concerning identified or identifiable natural persons".

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Categories of personal data which are considered sensitive in the Dominican Republic are: a person's political opinions, religion, philosophical or moral convictions, labor and union affiliation, and health and sexual information. Race it is not formally included, but is mentioned as an exception for health treatments and procedures (see (b) below).

As regards sensitive personal data, the Data Protection Law indicates that entities are obliged to obtain express, free, conscious consent to treat this kind of data; and treatment of such data is expressly forbidden without that consent.

There are two exceptions from the obligations regarding express consent and prohibition of treatment:

(a) Churches, religious associations, hospitals, political organizations and labor unions may collect such data in order to have a registry of their members.

(b) Data on health, "race" and sexual life may be treated when it is necessary for the prevention or for diagnosis of an illness, sanitary assistance or medical treatments or for the management of health services, provided that such data processing is carried out by a professional subject to professional secrecy.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The principles in data protection to be followed are:

(a) Consent must be obtained to use the data unless an exception applies;

(b) Lawful: personal data should not be kept or used for illegal purposes;

(c) Quality of data;

(d) Notification: All individuals should be informed of the following concerning their data:

  (i) purpose of its use,

  (ii) the existence of database, and

  (iii) the possibility of enforcing their rights of access, rectification and deletion of data;

(e) Data must be secure;

(f) Duty of confidentiality;

(g) Loyalty: Data must be collected in a legal manner; and

(h) Data collected must be appropriate, relevant and not excessive in relation to the specific, explicit and legitimate scope and purpose for which it has been obtained.

As regards exceptions from the need for consent, in the Dominican Data Protection Law regarding marketing and advertising issues, there is no mandatory requirement for prior consent for the transfer of the following types of personal data:

- data compiled from public sources, such as telecommunications lists (phone books);
- data for marketing purposes, such as name, ID number, passport, tax ID and any other biographic information;
- data from commercial, labor, contractual or scientific relation and are needed for the development and fulfilment of the duties;
- where an information dissociation procedure had been applied, so that the persons to whom the information refers were unidentifiable; and
- data from opinion polls, statistics, market and scientific investigations and research, when data does not identify a particular person, or make it easy to identify them.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

There is no obligation to have a data protection officer.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

At this moment in the Dominican Republic, there is no obligation to:

(a) have a privacy policy;

(b) appoint privacy officers;

(c) register with any authority; or

(d) carry out risk impact assessments.

Moreover, there are no obligations specific to advertising.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in the Dominican Republic? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The only mandatory standards and procedures are found in the banking system and also in the telecommunications sector. In 2020, the Dominican Republic is implementing security obligations to the banking system and credit bureau companies. There are no special regulations in any other sector, other than the general duty to maintain secure the data.

The general rule in the Data Protection Law is: "It is prohibited to record personal data in files, records or databanks that do not meet technical conditions of integrity and security". There is no legal definition of such "technical conditions", other than that referred to earlier with respect to the banking system.

6.2 How are data breaches regulated in the Dominican Republic? What are the requirements for responding to data breaches?

Outside the Banking system and credit bureau companies, there are no requirements for responding to data breaches and no sanctions for data breach incidents per se. There is only a general obligation on entities to preserve and protect the data and information in their systems.

There is no requirement to provide formal notice of data breach or security incident.

There is no sanction for the company from which the data breach occurred, but if the incident is a result of illicit access by an employee or a third party, the illegal penetration of the system, the use and exposition of the data is sanctioned by the Technology Crimes Law.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

All individuals have the right of access, rectification and deletion of data.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The Anti-Spam Law indicates expressly that users in the Dominican Republic have the right not to receive unsolicited commercial emails with advertising and offers (spam). Also, users have the right to reject spam emails and to opt out from any list they have previously consented to be on.

Companies have the right to send commercial/advertising/offers emails if there has been any sort of previous commercial relation with the customer. The mechanism to collect email addresses must be legal and transparent, as malicious collection of emails address is banned in the Dominican Republic. The user will always have the right to opt out.

Emails allowed by the Law must be clearly identified as "advertising" ("*publicidad*" in Spanish). Commercial messages also must comply with the obligation to identify the sender and include a valid email address to allow the recipient to send a message to opt out of further communications.

Note that these rules only apply to emails; social media is not included.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There are no special rules regarding cookies, pixels, SDKs.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There are no special rules. Compilation of addresses, direct advertising or sales and other similar activities is permitted, if data is taken from public sources or obtained with consent from the persons concerned, in order to establish profiles for promotions, advertising and consumer habits.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The sharing of data with third parties for customer matching is permitted and no further consent is necessary if there is consent to data processing.

8.5 Are there specific privacy rules governing data brokers?

There are no special rules for data brokers.

8.6 How is social media regulated from a privacy perspective?

There no special rules regarding social media.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are no special rules for loyalty programs and promotions.

The Consumer Protection Agency enforces data protection clauses in the rules of promotions, raffles and games.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

There is no prohibition or limit on the countries to which data may be transferred.

In the Dominican Republic the validity of transfer agreements or the Binding Corporate Rules are accepted and Sectoral and administrative agreements or business decisions are permitted.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

There are no special rules regarding data transfer other than that personal data may only be transferred internationally in the following circumstances:

(a) there has been formal authorization from the data subject;

(b) data for needed for medical treatment of epidemic investigation;

(c) banking transactions;

(d) transfer agreed in international and free treaty agreements;

(e) cooperation with international criminal investigations;

(f) fulfillment of a data protection agreement;

(g) judicial process, including tax and customs issues; or

(h) data transfer from a public registry, requested by an international institution with a legitimate interest.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The Data Protection Law has a wide provision whereby all violations of any of its provisions will be sanctioned with a prison term of between 6 months and 2 years and a fine of between 100 and 150 times the minimum wage. Such violations include:

(a) acting in bad faith, inserting false personal data in databases or providing false information to a third party;

(b) illegally accessing a data base; and

(c) revealing personal information included in a database to a third party.

The Banking Superintendence with authority as control agency to inspect the personal data processing of the information bureaus may impose fines up to US$30,000.

10.2 Do individuals have a private right of action? What are the potential remedies?

The Dominican Law admits the *Habeas Data* personal action to enforce the Data Protection Law. It entitles individuals to collect, rectify or delete their personal data.

The victims are entitled to collect 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 an information holder, after he/she has obtained a favorable pronouncement in a procedure followed in accordance with the provisions of the Data Protection Law; or

(c) violation in a serious or repeated manner of the provisions of the definitive sentences of the civil courts.

If the violation of privacy has been committed alongside a violation of the Cybercrime Law (eg, illegal access), penalties are much higher.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Dominican Republic which affect privacy?

Sadly, it is very common in the Dominican Republic that companies and government institution 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.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The Government is working on a new draft data protection law closely modelled on the European GDPR.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Dominican Republic?

In 2019, the Dominican Government enacted a law to protect the privacy and images of individuals involved (hurt or dead) in accidents (see question 1.2).

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The advances in contact (call) centers and outsourcing business, which have increased in the Dominican Republic, have shown that there is a need to implement stronger international rules of data protection through contracts.

12.2 What do you envision the privacy landscape will look like in 5 years?

Dominican people are taking conscience about privacy. In 5 years, it is likely to be better protected.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The existence of a government authority as data protection authority and the penalties or fines that it might be imposed.

ECUADOR

1 PRIVACY LAW

1.1 How is privacy regulated in Ecuador?

Ecuador does not have a Data Protection Law; however, the Constitution recognizes and guarantees the protection of personal data, establishing that the authorization of the data owner is necessary for any collection, filing or dissemination.

In addition to the constitutional regulations, there are regulations scattered in various legal instruments that refer to the protection of personal data for specific issues, with some inconsistencies and without procedural rules, such as the Organic Telecommunications Law, the Monetary and Financial Organic Code and the Public Data Registration Law.

Therefore, the absence of specific technical regulation on the matter and the lack of an expedited course of action to enforce rights, have left data privacy behind in Ecuador with almost an un existing actual protection to the data owner.

However, a specific Bill for the protection of personal data was presented by the Executive Branch to the National Assembly on September 19, 2019 which will regulate in detail this matter in a very similar way to the GDPR in Europe. This Bill may take several months more to be approved.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The laws that regulate data protection in Ecuador and are relevant here are the following:

(a) Constitution of the Republic of Ecuador, Articles 66(11), (19), (20) and 92: Article 66 recognizes and guarantees data protection. Article 92 determines that the authorization of the owner of the data is necessary, both in order for data to be collected and to be disseminated.

Problem: The Constitution of Ecuador recognizes the protection of personal data, without giving a specific definition, which leaves it open to interpretation as to ownership of the right. In addition, no competent authority is established to regulate or supervise compliance with the few existing rules on protection within the Ecuadorian legal system. This is left to a *habeas data* proceeding before a regular judge, which is not usually effective.

(b) Organic Law of Jurisdictional Guarantees and Social Control, Articles 49 and 51: In accordance with the Constitution, these contemplates the *habeas data* proceeding.

(c) Organic Law of Telecommunications, Articles 22, 24, 78, 80, 81 and 82: These Articles set out rules on the rights of customers using telecommunication services, the obligations of telecommunication service providers, the right to privacy and the commercial use of personal data.

(d) Organic Monetary and Financial Code, Articles 352–360: These develop some scarce regulation on the protection of personal information of users of the national financial system, which is managed by the financial institutions in Ecuador.

(e) Regulations for the Management of Confidential Information in the National Health System, Articles 17, 27 and 38: These contain some regulation on the matter; however, they confuse “confidential information” and “sensitive data”.

(f) Labour Code, Article 42(7): This imposes an obligation on employers to have and update their workers' data.

(g) Organic Code of the Social Economy of Knowledge, Creativity, and Innovation, Articles 140 and 141, General Provisions 26 and 27: These address personal data from an intellectual property point of view, stating that personal data is not part of the protectable matter of databases.

(h) Public Data Registration Law: This is not a personal data law, as it doesn't interfere with private databases. It does not define personal data and is limited to regulating the compilation of information contained in the different public offices.

(i) Comprehensive Organic Criminal Code, Articles 178 and 229: This typifies punishable activities regarding illegal database disclosure and violation of privacy, however, it confuses "confidential information" and "intimacy rights".

(j) Pronouncements of the Constitutional Court of Ecuador:

(i) Sentence No. 001-14-PJO;

(ii) Sentence No. 002-11-SIN-CC.

(k) Bill for Personal Data Protection: This was presented to the Assembly in September 2019; it clarifies the subject and all its concepts, becoming a comprehensive regulation with international standards.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Since Ecuador does not have a law for the protection of personal data, and the scattered regulations do not contemplate any specific proceedings, it is necessary to follow the provisions of the Constitution, which, through a *habeas data* proceeding, guarantee access to personal data, through which the owner of such information may request for it to be rectified, deleted or updated, or simply seek access to it.

The Organic Law of Jurisdictional Guarantees and Constitutional Control states that *habeas data* actions must be filed before the competent judge where the transgression takes place. Although it is not a complex proceeding, it is not simply an execution or compliance process, and may require a public hearing and the presentation of evidence.

The Bill for Personal Data Protection simplifies the situation and establishes a specific proceeding for this, which is handled through an administrative procedure before the Personal Data Protection Authority (which has yet to be created).

2 SCOPE

2.1 Which companies are subject to privacy law in Ecuador?

According to the Constitution, any entity, public or private, that handles information or personal data of any person, is subject to privacy rules.

2.2 Does privacy law in Ecuador apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Currently, in Ecuador, there is no specific rule about the scope of application of privacy laws; however, the Bill for Personal Data Protection will establish that it is applicable even when data processors are not domiciled in Ecuador, but the data owners are.

In addition, the Bill provides rules regarding data transfer to other countries (international transfer) in both the public and private sectors. Companies or economic groups must have binding corporate policies and regulations regarding data protection, which must be approved by the Authority.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Ecuador?

Although, Ecuador has various piecemeal rules on data protection, it does not have a specific rule that clearly defines what "personal data" really means and often confuses it with "confidential information" and "intimacy rights".

The Bill for Personal Data Protection, however, defines "personal data" as "data that identifies or makes identifiable a natural person, directly or indirectly, in the present or future". This definition includes metadata and data fragments.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" in Ecuador is treated in general by the Constitution as personal data that reveals racial, ethnic or religious origin, political positions, trade union membership, and data concerning health, sexual life or any other personal data that may cause discrimination in the life of the owner. There are no specific obligations regarding sensitive information.

The Bill defines "sensitive data" as data "related to ethnicity, gender identity, cultural identity, religion, political affiliation, judicial past, immigration status, sexual orientation, health, biometric data, genetic data and those whose improper processing may give rise to discrimination". In addition, the Bill opens up the possibility that the Personal Data Protection Authority may implement other categories of sensitive data.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The primary source of the principles governing data privacy are set out in Article 92 of the Constitution of Ecuador, which contains various rights for data owners, which companies must respect in the processing of information.

Transparency: All persons have the constitutional right to know about the existence of any data about them that is being held in both public and private companies, as well as its usage. This principle is based on the consent of the owner. One example of the transparency principle is in Article 79 of the Telecommunications Law, which establishes that, in the event of a particular risk of a breach of the security of the public network or the telecommunications service, subscribers must be informed and the necessary measures must be taken to avoid the damage.

Purpose limitation: For example, Article 82 of the Telecommunications Law determines that companies that provide telecommunications services may not use personal data of customers without prior express consent, which should specify what data and information may be used and for how long and for what purpose.

Security: Article 74 of Telecommunications Law establishes a series of technical security and invulnerability measures that companies must follow for the use of personal data and information. The main objective of this is to preserve the right to privacy mentioned in the Constitution. Similarly, Article 80 establishes the obligation on telecommunication companies to implement internal procedures to deal with requests for access to personal data and the supervision and control thereof, following the provisions of the Agency for Regulation and Control of Telecommunications.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

As mentioned before, at this time there is no Privacy Law that specifically regulates the roles of companies with respect to personal information/personal data.

However, in the Bill currently being discussed by the Assembly, roles are established for both, those in charge and those responsible for the processing and protection of personal data affecting their obligations, for instance:

(a) **Obligations of data controllers**: Article 71 of the Bill establishes a series of obligations that the data controller will have to comply with, ranging from technical requirements to the need to sign confidentiality contracts and permanent updating and registration.

(b) **Obligations of Obligations of data processors**: Article 72 of the Bill contains the roles of the data processor, which relate mainly to the security measures to be implemented.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

At present, there is no Privacy Law that specifically regulates the key obligations with a focus on advertising, but, throughout the Bill, obligations are imposed on the handling of data, specifying that use is limited by the consent of the owners. Without the consent of the data owner, information cannot be treated, used or transferred.

Under the Bill, the obligations imposed on the controllers and processors include, amongst others, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, and registering with a privacy authority.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Ecuador? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

As stated above, data security regulations are dispersed within the Ecuadorian legal system.

Some of the standards that contain minimum regulatory parameters are:

(a) Paragraph 19 of Article 66 of the Constitution (in force since 2008) stipulates the right to the protection of personal data. However, it is not yet regulated, as in two other countries in the region: Venezuela and Bolivia.

(b) Article 229 of the Comprehensive Organic Criminal Code punishes with one to three years of prison anyone who discloses data that "violates the secrecy, intimacy, and privacy of individuals". If the person is a public servant or bank employee, the penalty is three to five years.

(c) Article 360 of the Organic Monetary and Financial Code prohibits the commercialization of credit references. The Superintendence of Banks has until September to assume the management of these records.

6.2 How are data breaches regulated in Ecuador? What are the requirements for responding to data breaches?

Currently, in Ecuador, there is no clear and specific procedure for responding to security breaches. In principle, an investigation of the facts is initiated by the Attorney General's Office and, subsequently, the possible actions to be presented are analyzed following the criminal proceedings and regulations established at the time.

On September 16, 2019, Ecuador was the victim of a massive exposure of private data of more than 20 million of its citizens by a company called Novaestrat, which led to questioning and evaluating the actions being taken to protect this type of information.

In the case of Novaestrat, the damage was caused by a security incident due to a bad configuration of a database. It is important that companies not only dedicate time and resources to the technological aspects of security, such as encryption solutions or prevention of information leaks, but also to the development of processes and security policies that include appropriate controls and contribute to the proper management of security.

This case was the catalyst for the Bill for Personal Data Protection to be sent to the Assembly for approval.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The Ecuadorian legal system, specifically the Constitution, states that persons have the right to know of the existence of and have access to their data held by public and private entities. Also, it grants citizens the right to know the use, purpose, origin, and destination of their information, plus the duration of the file or data bank, the rectification of data and the requirement of authorization of any data transfer. Personal data protection is a Constitutional right; and so use of personal data must respect the owners' honor and full enjoyment of their rights.

The Telecommunications Law determines that providers of telecommunications services must adopt appropriate technical and management measures to preserve the security of their network in order to ensure the protection of personal data. It also grants to the data owner the right of access to such data without cost, to update his/her own data, as well as request its elimination or annulment.

If the constitutional rights of data owners are not respected, those affected may file habeas data actions, in accordance, with Article 50 of the Organic Law of Jurisdictional Guarantees and Constitutional Control.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Currently, Ecuador does not have a specific law regulating marketing communications, but it is expected that once the Bill for Personal Data Protection is approved, a specific regulation on this matter will be developed by the Personal Data Authority.

8.2 How is the use of tracking technologies (eg, cookies, pixels, sdks) regulated from a privacy perspective?

As stated above, this is not currently regulated Ecuador but a specific regulation is expected to be developed when the Bill on Personal Data Protection is approved by the Assembly.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There is no current regulation on the matter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook custom audiences or via LiveRamp) ?

The only clear limit that has been defined in the Ecuadorian legal system on personal data is the consent of the owner for collection, use and transfer of personal data. This means that, currently, advertisers require express authorization to share a person's data for customer matching.

However, the Bill is more permissive, as it states exceptions from the need to obtain the owner's consent for transferring data, such as when the data has been collected from sources accessible to the public, or when the data treatment corresponds to the legal relationship between the data owner and the data controller.

8.5 Are there specific privacy rules governing data brokers?

There is no current regulation on the matter.

8.6 How is social media regulated from a privacy perspective?

There is no current regulation on the matter; all provisions focus more on the constitutional right of intimacy of the person.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There is no current specific regulation on the matter. However, it is not possible to collect, use, process or transfer any personal data for any purpose without the authorization of the owner.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Currently, any data transfer requires the express consent of the owner, according to the Constitution. Hence, the first restriction is the consent of the owner, which must given be prior to transfer and expressly specify the information that is being authorized to be transferred.

However, in Article 48 of the Bill, exceptions are set out when the consent of the holder for the transfer or communication of personal data will not be required. These include, among others:

(a) when the data has been collected from sources accessible to the public,

(b) when personal data must be provided to an administrative or judicial authority, and

(c) personal data related to health necessary to solve an emergency.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

The main consideration for companies is consent of the data owners. In addition, the Bill establishes that the processing of personal data that is carried out by third parties must be regulated by contract, that clearly and precisely establishes that the data processor will treat the personal data according to the instructions of the data controller and that data will not be used for purposes other than those stated in the contract.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

As mentioned above, there is no specific law in Ecuador that provides sanctions in cases of violation of the information and personal data of citizens. However, at present, the Comprehensive Organic Criminal Code establishes the following:

> "**Article 178 — Violation of privacy -** Any person who, without the legal consent or authorization, accesses, intercepts, examines, retains, records, reproduces, disseminates or publishes personal data, text, voice, audio and video messages, postal objects, information contained in computer media, private or confidential communications of another person by any means shall be subject to a custodial sentence of one to three years..."
>
> "**Article 229 — Illegal disclosure of database -** Any person who, for his own benefit or that of a third party, discloses registered information contained in files, archives, databases or similar media, through or directed to an electronic, computer, telematics or telecommunications system; voluntarily and intentionally materializing the violation of the secrecy, intimacy and privacy of persons, shall be punished with a custodial sentence of one to three years..."

Also, there is limited case law of damages awards based on *habeas data* resolutions if actual harm to the data owner is demonstrated.

10.2 Do individuals have a private right of action? What are the potential remedies?

In accordance with the Constitution of Ecuador and the Organic Law of Jurisdictional Guarantees and Constitutional Control, the owners of information and personal data that have been affected may file a habeas data action on their own rights the same regarding the couple of criminal regulations on the matter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Ecuador which affect privacy?

There are no specific rules yet.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The Bill for Personal Data Protection, as mentioned before, should be approved by the Assembly in the following months and will establish a complete and highly regulated legal frame for data processing.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Ecuador?

Not at this time.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Data protection is a very new topic for Ecuador; it gained some relevance when it was included in the Constitution of 2008; however, it was never properly regulated. The lack of a specialized Law that clarifies the ambiguities in the dispersed laws and fills the legal voids is the main reason that led the proposed Bill in 2019.

Nevertheless, the massive data breaches which have been publicly reported demonstrate how carelessly data processing is being handled in the country and reveal the weakness of our security systems, and are the main trigger for the Bill to be finally presented to the Assembly.

My personal opinion is that this law is needed in Ecuador now with more urgency than ever before. Perhaps the Bill presented to the Assembly could be deemed a little over-regulatory; however, this is necessary for a country in which we have been absolutely unprotected.

12.2 What do you envision the privacy landscape will look like in 5 years?

I believe that the Bill is a response to the lot of legal gaps that exist in Ecuador on the processing of personal data. If the Bill is accepted and, subsequently, the creation of a Regulation of the Law of Protection of Personal Data is considered, the panorama in five years in Ecuador will be different. That is, the answers to data protection problems will be agile, clear and fast. The security measures for data protection will be effective, and, above all, there will be clear limits on the use and processing of personal information. The

country by then will most likely have a "formal" control of data processing and protection of privacy rights, which, of course, will still be imperfect due to the lack of experience of the Authority (to be created) and the compliance timeframes that will have to be granted to the companies.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

If the Bill is approved, the establishment of responsibilities and roles (data controllers and delegates) for processing personal data will definitely represent challenges for companies. This because, as there is a specific rule that regulates the responsibilities of each of the subjects involved, it means that companies will have to use more resources to comply with these legal requirements, which they are not used to. Likewise, investment in better developed terms and conditions of use, security measures and registration of data bases will be new challenges for companies in Ecuador.

EGYPT

1 PRIVACY LAW

1.1 How is privacy regulated in Egypt?

Privacy in Egypt is governed mainly by the new Egyptian constitution, which was adopted in a referendum in January 2014. Egypt is also in the process of issuing a new Data Protection Law. In August 2018, the Egyptian Cabinet approved a draft for the proposed Data Protection Law, which still awaits approval by an open session of Parliament.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Article 57 of the newly adopted Egyptian Constitution stipulates that: "Private life is inviolable, safeguarded and may not be infringed upon. Postal, telegraph, e-correspondence, telephone calls and any other means of communications are inviolable and their confidentiality is guaranteed and they may only be confiscated, examined or monitored by causal judicial order, for a limited period of time, and in cases specified by the law. The state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law".

Article 99 of the Constitution specifies that: "... any assault on individual freedom or the inviolability of citizens' private lives and any other public rights and liberties guaranteed by the Constitution shall be considered a crime".

Egypt is part of the following regional and international conventions:

(a) The Universal Declaration of Human Rights;

(b) The International Covenant on Civil and Political Rights;

(c) The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families;

(d) African Charter on Human and People's Rights;

(e) African Charter on the Rights and Welfare of the Child;

(f) The United Nations Convention Against Transnational Organized Crime;

(g) The Cairo Declaration on Human Rights in Islam.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Currently Egypt does not have regulatory bodies to enforce privacy law matter. We expect this to be resolved with the issuance of the new data protection law's executive regulations.

2 SCOPE

2.1 Which companies are subject to privacy law in Egypt?

Laws related to data protection and privacy are applicable to all natural and legal persons in Egypt.

2.2 Does privacy law in Egypt apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No data privacy law exists in Egypt as of yet, thus this does not apply.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Egypt?

In Egypt, personal information/data, which appears on an individual's passport, includes: the passport number, the individual's photo, the individual's full name, gender, nationality, national ID number, marital status, profession, military status, postal address, place and date of birth of the passport holder.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

In Egypt, the following categories are considered sensitive personal information:

(a) mental, psychological, or physical health;

(b) genetic data;

(c) biometric data;

(d) financial data;

(e) religious beliefs;

(f) political opinions;

(g) criminal records;

(h) children's data.

At the moment, there are no obligations around the collection of sensitive information; however, it is expected that this matter will be covered in the new data protection law.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

In 2006, the Egyptian government enacted the Egyptian Consumer Protection Act, which does not govern the protection of consumers' personal data and information. The current Act does not offer a transparency mechanism which would determine who should process the personal information of consumers as well as the means by which they will be able to apply the rights of information. This may all change with the issuance of the new privacy law.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No data privacy law exists in Egypt as of yet, thus this does not apply.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

No data privacy law exists in Egypt as of yet, thus this does not apply.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Egypt? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Presently, data security is not currently regulated in Egypt due to the lack of a data protection law. That being said, according the draft data protection law, which should be issued before the end of 2020, the processor of data is required to notify the national regulator within 48 hours, as soon as they become aware of any personal data security breach. See, further, question 5.2 as to the notification.

6.2 How are data breaches regulated in Egypt? What are the requirements for responding to data breaches?

Under the suggested draft privacy law in Egypt, the individual or entity that controls or processes the data must, upon knowing of any data breach, inform the national regulator within a timeframe of 48 hours. This notification must also:

(a) outline the data breach and the estimated number of data subjects and records involved;

(b) contain the responsible officer's name and contact information;

(c) explain the possible and most expected penalties resulting from the data breach

(d) describe the proposed measures with which the controller plans to address the data breach; and

(e) document any data breach, as well as the action taken to remedy such breach.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

At the moment, this is not clear, but it is expected to be covered in the executive regulations of the new data protection law.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Emails, text messages and push notifications are not yet governed in Egypt by any laws or legislation from a privacy perspective.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Tracking technologies are not yet governed in Egypt by any laws or legislation from a privacy perspective.

8.3 How is targeted advertising and behavioural advertising regulated from a privacy perspective?

Targeted advertising and behavioural advertising are not yet governed in Egypt by any laws or legislation.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Customer matching is not yet governed in Egypt by any laws or legislation.

8.5 Are there specific privacy rules governing data brokers?

There are currently no rules or laws that govern data brokers in Egypt.

8.6 How is social media regulated from a privacy perspective?

During mid-2018, the Egyptian Parliament approved new legislation, the Media Regulation Law, which restricts the freedom of expression on online platforms for users having more than 5,000 followers, and makes them subject to the same regulations as those imposed on journalists and established media companies.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are currently no rules or laws that govern loyalty programs and promotions in Egypt from a privacy perspective.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

There are currently no laws restricting the transfer of data offshore. This may change when the new data protection law is eventually issued.

Under the current draft law, a controller can transfer data to another controller outside abroad subject to the following:

(a) the controllers settle on the nature of work and the purpose of the transfer of the relevant personal data;

(b) the controllers both have an authentic interest in said personal data; and

(c) the controller located outside of Egypt is required to have the same legal/technological protections as the ones available in Egypt.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Under the draft privacy and data protection law, a controller can provide the personal data to another controller abroad given the following conditions:

(a) The controllers have reached an agreement regarding the nature of work as well as the purpose of the personal data;

(b) The controllers both have a genuine interest and concern in the data; and

(c) The controller located abroad at least must have the same legal/technological defences as available in Egypt.

Furthermore, data transfers to foreign countries are against the draft law, unless the transfers are to countries that afford the same protections as those under our draft law. Transfers will be exempt from the conditions above in cases where the following applies:

- for the protection and safety of the data subject's life for the provision of medical care, treatment, or the administration of medical services;
- for the proof, exercise, or defending a judicial right;
- to execute a procedure as required by an international judicial agreement;
- to protect the public interest; or
- to complete a bank wire transfer.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Article 113 of the Egyptian Criminal Code No. 58/1937 imposes criminal penalties on unauthorized collection of photographs or recordings of individuals in private places. Furthermore, article 309-bis of the Criminal Code states that: "a penalty of detention for a period not exceeding one year [...] inflicted on whoever encroaches upon the inviolability of a citizen's private life, by committing one of the following acts in other than the cases legally authorized, or without the consent of the victim:

- eavesdropping, recording, or transmitting via any instrument whatever its kind, talks having taken place in a special place, or on the telephone;
- shooting and taking or transmitting by one of the instruments, whatever its kind, a picture of a person in a private place".

It is expected that more penalties will be imposed with the issuance of the imminent privacy and data protection law.

10.2 Do individuals have a private right of action? What are the potential remedies?

This is not currently addressed by the current laws and it is expected to be addressed with the issuance of the new data protection law.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Egypt which affect privacy?

Not applicable.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Egypt is planning to issue a new data protection and privacy law within the upcoming year.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Egypt?

None.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

As mentioned, the biggest change has been the draft data protection law that was completed in 2018. We believe that the pressure of international laws and regulations is what triggered these changes in Egypt.

12.2 What do you envision the privacy landscape will look like in 5 years?

We believe that the issuance of the new data protection will change the landscape drastically over the next five years. Egypt is typically not so concerned about data protection, so the fact that it has already taken a step forward in this sense is a significant move. We expect that regulations similar to those imposed on EU countries by the GDPR will also be implemented on those companies incorporated in Egypt which by nature collect customer private data. It will be interesting to see how the new law will be implemented and also to understand the executive regulations which shall govern this law with more accuracy.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

N/A

EL SALVADOR

1 PRIVACY LAW

1.1 How is privacy regulated in El Salvador?

El Salvador does not have a specific privacy law; however, privacy information is regulated in several laws that are in effect in El Salvador.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Privacy is regulated in the following Laws:

(a) Constitution of El Salvador;

(b) Special Law Against Computer and Related Crimes;

(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; and

(g) Law on the Supervision and Regulation of the Financial System.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

In El Salvador there is not a specific privacy law, and so the entities in charge of regulating privacy will depend on the case in hand, eg the Superintendence of the Financial System and the Consumer Advocacy is the regulatory entity in the cases of banks.

2 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No, privacy law in El Salvador does not apply to companies outside the country. However, it does apply to the foreign corporations that operate in the country.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive personal information" is information that relates to a person's creed, religion, ethnic origin, affiliation or political 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, to personal and family privacy.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The key privacy principles are:

(a) Responsibility and Security: the data subject should be secure that the company is using its information pertinently;

(b) Purpose: data should only be used for the purpose stated or for what was requested and not for any other purposes;

(c) Consent: data should not be disclosed without the consent of each individual providing their data; and

(d) Access: individuals who provide data should be allowed to access their data and make corrections to any inaccurate data.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Yes, banks are the best example of this, in that they have to request authorization from the Superintendence of the Financial System (controller) to provide information on deposits and accounts, as this is information that can only be given to its owners.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The key obligations required by privacy law are:

(a) to inform or provide information to a client who requests their information;

(b) to provide the information required by the competent authorities; and

(c) when a data information agency for any reason finishes its operations in the country, it must send its database to the Superintendence of the Financial System.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in El Salvador? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

In general, there is no minimum standard for data security, because each institution has a specific law that regulates it, for example, banks are regulated by the Bank Law and the Law on the Supervision and Regulation of the Financial System.

6.2 How are data breaches regulated in El Salvador? What are the requirements for responding to data breaches?

It depends 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 cybercrimes. In addition, the Criminal Code regulates some breaches, and provides sanctions.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The Law on the Regulation of Information Services on People's Credit History provides that individuals can modify or add to their personal information. Where those who have a bad credit record manage to pay their debt, companies have to remove them from the list of "not subject to credit" and pass them to the list of "subject to credit" within a set time frame.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

There are no regulations regarding privacy in marketing communications.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There are no regulations regarding privacy and tracking technologies.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There are no regulations regarding privacy and advertising and behavioral advertising.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

There are no regulations regarding privacy and sharing data with third parties for customer matching. However, when individuals sign a contract with a company, the company is allowed to use their information in order to promote and share content or campaigns with others.

8.5 Are there specific privacy rules governing data brokers?

There are no regulations regarding privacy and data brokers.

8.6 How is social media regulated from a privacy perspective?

There are no regulations regarding privacy and social media; however, when individuals sign a contract with a company to promote and regulate their social media, they are giving the company full access to information.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are no regulations regarding privacy in loyalty programs and promotions. However, a privacy clause will be included when the company in charge of the program enters into a contract with other companies, establishing that they are not allowed to sell or use the information provided (database) for purposes other than loyalty programs or promotions and for the contract purposes.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

In accordance with the Bank Law, companies that form part of a financial conglomerate can share customer databases. Each of the companies that are part of the conglomerate may make economic information available to other financial entities regarding their customers, mostly in regard to their credit background, with previous authorization of the Superintendence of the Financial System.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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, the data transfer is done by cooperation, and mostly 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 involved in some type of criminal act, they need to exhibit the information contained in databases in the procedure.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

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 individuals have a private right of action? What are the potential remedies?

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 breaches 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 Bank 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of El Salvador which affect privacy?

As a constitutional precept, no one can do anything to adversely affect others "since my right ends where the other's right begins". Data information is considered personal and no one can disclose that information unless they have the consent of the owner to do so. Culturally, we have tried to safeguard the rights of integrity and property, which include personal information and personal data.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Yes, there is a group that is studying and elaborating a preliminary draft Data Protection Law whose purpose is to delineate privacy limits for the use of personal data and its ownership. This is because, even though there are some laws that regulate privacy issues (see question 1.2), a specific law is needed that will regulate data in general, setting out provisions as to specific permissions, restrictions, obligations, as well as sanctions, remedies, etc.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in El Salvador?

No, since El Salvador does not have a specific Data Privacy Law.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

In El Salvador, we have realized that there is a need for data to be protected by a specific law, and this is why a preliminary draft Bill is being created and studied in order to pass the Bill to the Legislative Assembly for its approval.

12.2 What do you envision the privacy landscape will look like in 5 years?

Currently, there is no consolidated legislation that deals with data protection, but there is a preliminary draft Data Protection Bill, that would simplify matters both for individuals to know the rights they have and to regulate corporations to make proper use of personal data. The draft Bill also aims to periodically encourage companies and individuals to obtain the maximum benefits from the digital market, economic growth, innovation and government collaboration, marking the boundaries between privacy, use of personal data and their ownership.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The constant updating of the law may be the biggest challenge, since whenever a new regulation enters into force corporations must make a change of structure so as not to be involved in some type of infraction and often they need to take courses to learn about the new legislation and the best way to incorporate the changes in the laws in their business.

EUROPEAN UNION

1 PRIVACY LAW

1.1 How is privacy regulated in the European Union Member states?

Privacy is regulated on two levels: that of the European Union and that of the Member states.

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 as far as the processing of personal data is concerned.

The protection of personal data is also enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. According to Article 51 of the Charter of Fundamental Rights, all the institutions, bodies, offices and agencies of the European Union are bound by it. Also, the Member states are addressed by the provisions of the Charter and 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.

On the EU level there is also the ePrivacy Directive which is not directly applicable but obliges the Member states to implement its regulations into national law. Currently, a draft of an ePrivacy Regulation is being deliberated and will, probably in the near future, replace the ePrivacy Directive. Once in force, it will be directly applicable in the 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.

At the end of this chapter, the national laws of the Member states will be dealt with separately for each country.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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, via the treatment, security and storage until their 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 this chapter, references to "Articles" are to Articles of the GDPR.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

According to Article 51 onwards, each Member state has to establish its own independent supervisory authority. Such authority's main task is to monitor and enforce the application of the GDPR. In order to do so, the GDPR requires the Member states to provide their supervisory authorities with great investigative powers. The GDPR contains a framework of sanctions to be applied by the Member states but does not itself contain any enforcement stipulation. The GDPR is therefore enforced by the Member states themselves. In order to ensure uniform application of the GDPR, a Data Protection Board has been set up at EU level. The Board is composed of the head of one supervisory authority of each Member state.

In addition to the supervisory authority, it is possible, at the level of the Member states, that certain aspects of the protection provided by the GDPR can be pursued and enforced by the courts of the Member states upon the request of competitors, consumer protection associations or the data subjects themselves.

2 SCOPE

2.1 Which companies are subject to privacy law in the European Union?

According to Article 2, 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 EU privacy law apply to companies outside the European Union? If yes, are there specific obligations for companies outside the European Union (eg, requiring a company representative in the European Union)?

Yes, it can apply to companies outside the European Union. The territorial scope of the GDPR is stipulated in Article 3:

(a) The GDPR applies to 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) It applies to 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 their 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 INFORMATION

3.1 How is personal information/personal data defined in the European Union?

Under Article 4, "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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Special categories of personal data are covered in Article 9, which 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 expressively 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. A child must be at least 16 years old to give valid consent to the processing of his/her 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The key principles that have to be applied when processing personal data are stated in Article 5, which states that personal data must be:

- processed lawfully, fairly and transparent — "lawfulness, fairness and transparency";
- collected with purpose limitation — "purpose limitation";
- adequate in relation to the purposes — "data minimization";
- accurate — "accuracy";
- kept for no longer than necessary — "storage limitation"; and
- processed in a manner that ensures appropriate security and protection — "integrity and confidentiality".

The controller shall also be responsible for, and be able to demonstrate compliance with, the key principles ('accountability'). A further key principle is the information obligation vis-à-vis data subjects and authorities.

Regarding lawfulness, a fundamental principle is set out in Article 6(1). This states that data processing is prohibited except where it is explicitly allowed by law, namely if:

(a) the data subject has given consent to the processing of his/her personal data for one or more specific purposes;

(b) the 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) the processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) the processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) the 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; or

(f) the 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, in particular where the data subject is a child.

Consent as a basis for the processing of personal data is defined in Article 4(11). The requirements for a valid consent are regulated in Article 7. The consent has to be an unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data. That means on the one hand, that consent has to be given in an active way. On the other hand, it means that it is, in principle, not bound to a formal regulation. But the form should be chosen in such a way that the controller can fulfil his duty of proof under Article 7.1. In case consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

The consent has to be freely given, specific and informed. When assessing whether consent is freely given, the utmost account is taken of whether, inter alia, the performance of a contract/provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. For consent to be specific it is necessary that the data subject can detect who processes what personal data about him/her and for which purpose(s).

The data subject has to be informed about his or her right to withdraw his or her consent at any time. If the data subject withdraws his or her consent, the processing of personal data must be stopped immediately. But the withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

There are two different roles a company processing personal data can take up:

(a) **controller**: who determines the means and the purpose of the data processing; or

(b) **processor**: who processes data on behalf of a controller.

A controller may only use processors which provide sufficient guarantees to implement appropriate technical and organizational measures so that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. A processing agreement needs to be in place regulating the obligations of the processor. When two or more controllers jointly determine the purposes and means of processing, they are joint controllers and need to execute an agreement in order to protect the data subject's rights and to specify their respective tasks and roles to that respect.

Therefore, it is crucial to determine the roles of the companies processing the personal data because the required tasks and measures differ, depending on the role of the company.

Note that, in addition to the requirements resulting from its respective role, each company is responsible for its own compliance with the GDPR, including the responsibility of (joint) controllers for all information obligations vis-à-vis the data subject.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

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). The obligation requirements are stipulated in detail in Articles 13 (where collected from the data subject) and 14 (where not obtained from the data subject), which can serve as a guideline. 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 as stipulated in Article 30. Records must be in writing (which includes electronic form).

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in the European Union? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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 Article 32 of the GDPR and in national laws.

National data protection authorities have issued guidelines on data security (see the respective national chapters below).

6.2 How are data breaches regulated in the European Union? What are the requirements for responding to data breaches?

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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

A data subject has rights regarding the processing of his/her personal data (Articles 15–22). The rights are:

(a) **Access**: A data subject has the right to be told whether or not a controller has personal data concerning him/her, and, where that is the case, details about such data. This means, that any data subject can ask any company if it has information stored about him/her, even if no prior contact had been made. A controller is required to provide information in response to a request without undue delay, and in any event within one month of receipt of the request.

(b) **Rectification**: A data subject has a right to obtain from the controller without undue delay the rectification of any incorrect personal data.

(c) **Erasure**: A data subject has the right to erasure ("right to be forgotten"), meaning that a controller is obligated to erase personal data without undue delay under certain circumstances.

(d) **Restriction of processing**: A data subject has, under certain circumstances, a right to restriction of processing.

Where any rectification or erasure of personal data or restriction of processing has been carried out, the controller has the duty to communicate this fact to everyone to whom the personal data had previously been disclosed. The controller must inform the data subject about those recipients if the data subject requests it.

(e) **Data portability**: On request, a controller must provide a data subject with his/her personal data in a structured, commonly used and machine-readable format. The data subject also has the right to transmit such data to another controller without hindrance from the controller to which the personal data has been provided. This right is limited to data provided by the data subject to the controller.

(f) **Object**: A data subject has the right to object at any time to the processing of his/her personal data which was based on Article 6(1)(e) (necessary for the performance of a task carried out in the public interest) or Article 6(1)(f) (for the purposes of the legitimate interests pursued by the controller or a third party). Where objection is made, the controller may only carry on processing the subject's data if he/she can demonstrate compelling legitimate grounds for doing so, which override the interests, rights and freedoms of the data subject. The right to object can also be overridden for the establishment, exercise or defense of legal claims. In addition, a data subject can always, and at any time, object to the use of his/her personal data for direct marketing purposes.

(g) **No to automated processing**: A data subject also has the right not to be subject to a decision based solely on automated processing, including profiling.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The GDPR only regulates the processing (use) of the personal data, while national laws may regulate the permissibility and the means and prerequisites of commercial communications. See the national section on each Member state for details.

Purely from a privacy perspective, the general rules apply, namely that the processing (use) of personal data for marketing communications is permitted on the basis of (informed) consent or legitimate interests, both of which need to be documented. The general information requirements must be complied with.

In addition, the controller (or the processor) must inform the data subject, at the time of first communication with him/her, if not before, of the right to object to the processing of his/her personal data for the purpose of direct marketing. Where objection is made, the processing of the personal data for the purpose of direct marketing must cease, which means that any form of direct marketing must stop immediately upon the request of the data subject (Article 21).

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

(a) **General**: As with any personal data, the use of tracking tools is prohibited unless the processing of data can be based on a legal exemption (see question 3.3). As a result, only consent and legitimate interests can legitimize the use.

In addition, please note that, according to the ePrivacy Directive, the rules relating to tracking tools are not limited to personal data but cover all data which are being tracked (eg traffic data).

(b) **Cookies**: Regarding cookies, the European Court of Justice ("ECJ") has recently issued a decision from which some guidance regarding the consent can be obtained (Case No C-673/17). An effective consent requires an unambiguous action of confirmation, eg actively clicking a box affirming the consent on the website. In contrast, a box that is already checked off 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.

An exemption from the consent requirement in Article 5 of the ePrivacy Directive is made for technical storage that is strictly necessary in order to provide the website service explicitly requested by the user of a website. This exempts, eg, cookies that are implemented for the provision of a shopping cart function in an online shop. In contrast, cookies that are used in the context of tracking and analysis tools are not absolutely necessary for the operation of the website and, therefore, require consent.

(c) **Pixels and SDKs**: Regarding pixels, depending on the type of pixel used, use may be based either on consent or legitimate interests (see question 3.3). In any case, the information obligation of Article 13 has to be observed. The same applies to SDKs. However, as far as profiling is concerned, it is most likely that only consent will serve as a basis for processing the personal data.

(d) **Tracking tools operated by third parties**: As far as the tracking tools are operated by third parties which process that data, data controllers and processors need to sign either a processing agreement or a joint controllership agreement depending on their respective responsibility.

For embedding of third-party services (like Google Analytics), where the third party uses the personal data for its own purposes, the consent of the data subject is needed.

In this regard, it should especially be noted that the use of such a service requiring consent is only permissible if the consent has effectively been issued by the respective user prior to any personal data being collected. Until this time, processing may not occur, and a cookie that requires consent may only be set after consent has been issued. However, as far as Google Analytics is concerned, Google does not disclose what data they collect and what they use the data for. Therefore — at least according to the German supervisory authorities — a valid consent is currently not possible, because accurate information cannot currently be provided. For other tools this must be checked thoroughly in each case.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The sharing of data will be legal only when based on a legal exemption, of which consent or legitimate interests are most relevant (See question 3.3). The general information obligations in Articles 13 and 14 also apply (see question 5.1).

Facebook Custom Audience has to be differentiated:

(a) In the case of Facebook Custom Audience via the customer list, Facebook is the processor. Therefore, the controller and the processor (Facebook) need to have a processing agreement in place (Article 28).

(b) In the case of Facebook Custom Audience via the pixel method, Facebook and the provider are joint controllers. They need to have a joint controller agreement (Article 26).

In the case of using LiveRamp, a joint controller agreement is needed.

8.5 Are there specific privacy rules governing data brokers?

There are no specific rules governing data brokers in the GDPR. The processing of data will be legal only when based on a legal exemption, of which consent or legitimate interests are most relevant (see question 3.3). The restrictions of Article 9, regarding sensitive data, apply.

The information obligations of Article 14 must be observed where personal data has not been obtained from the data subject. In particular, it is necessary to clarify from which source the personal data originates, and, if applicable, whether it came from publicly accessible sources. Where personal data is collected from the data subject, the information obligations of Article 13 must be observed.

8.6 How is social media regulated from a privacy perspective?

Operators of social media are subject to the rules of the GDPR in the same way as anyone else. No special rules apply. It has to be pointed out, though, that website operators that use social media and social media operators may be considered joint controllers and thus would need a joint controllership agreement which complies with the requirements of Article 26.

According to an ECJ decision of June 2018 (Case No C-210/16), operators of Facebook fanpages in the European Union are joint controllers together with Facebook Ireland. Thus, a joint controllership agreement must be in place.

According to an ECJ decision of July 2019 (Case No C-40/17), the operator of a website that uses a social plugin causing the browser of a user of that website to transmit personal data of the user to that provider (eg, the Facebook "like" button) can be considered to be a controller. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue.

It is important to note that the requirements for a valid basis for the processing of personal data such as, eg, consent or legitimate interests must exist before the social plugin even starts processing (ie, collecting) the personal data from the user. This means that in cases where a consent is required because of the use of cookies, the social plugin must be inactive until such consent is validly issued. Technically, this can be implemented, eg, with the so-called "two-click" solution. The "two-click" solution means that the user, before activating the plug-in with the first click, will be informed, so that a valid consent can be granted. No data must be processed before this activation. Only after this first click the user can click the social plug-in (eg, the "like" button).

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are no special rules. The GDPR applies, and thus a legal basis for the use of the data must be available (see question 3.3). Certain information requirements apply.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Any transfer within the EU is subject to the general rules of the GDPR, ie, it must have a legal basis (Article 6, as to which see question 3.3) and comply with all the other requirements regarding data security etc. This also applies to a transfer between group companies.

In addition, in case of any transfer of personal data outside the EU the following has to be observed:

(a) **Transfers on the basis of an adequacy decision** (Article 45): A transfer of personal data may take place where the European Commission has decided that the third country ensures an adequate level of data protection. Currently, the European Commission has issued an adequacy decision regarding the following countries: Andorra, Argentina, Canada, Guernsey, Faroe Islands, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

Special case EU-US Privacy Shield: The treaty between the EU and the USA consists of an adequacy decision of the European Commission and different attachments, such as the so-called "Privacy Principles" (that regulate, in particular, the principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement and liability) and Letters of different US ministries, in which they commit themselves to comply with the standards. US-American companies may undertake to the US Department of Commerce to adhere to the Principles. Therefore, they have to publish a "Privacy Policy" that matches with the Principles and certify themselves. The self-certification has to be repeated yearly. Furthermore, they have to document the adherence. The companies that fulfil the conditions of the Privacy Shield are listed under https://www.privacyshield.gov/list.

For all US companies in the US not participating in the Privacy Shield one of the appropriate safeguards of Article 46 must be in place.

(b) **Transfers subject to appropriate safeguards** (Article 46): In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and only if enforceable data subject rights and effective legal remedies for data subjects are available.

The most relevant appropriate safeguards are the standard data protection clauses adopted by the Commission or by a supervisory authority and approved by the Commission.

(c) **Derogations for specific situations** (Article 49): In the absence of an adequacy decision or of appropriate safeguards, a transfer of personal data to a third country may take place only on one of the following conditions:

(i) Explicit consent of the data subject: 'Explicit' means that an implied consent is not possible. Furthermore, the data subject has to be informed about the possible risks of transfers due to the absence of an adequacy decision and appropriate safeguards;

(ii) The transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the data subject's request; or

(iii) 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;

(iv) The transfer is necessary for important reasons of public interest;

(v) The transfer is necessary for the establishment, exercise or defense of legal claims;

(vi) 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; or

(vii) The transfer is made from a register which, according to EU or Member state law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member state law for consultation are fulfilled in the particular case.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

There are no privileges for transfer between group companies, which are considered independent and separate entities under the GDPR. Therefore, a legal basis under the GDPR must be in place for each inter-group transfer of personal data.

It should be noted that a joint controllership or a processing agreement may be necessary in certain circumstances. It depends on which role the respective group company takes on in processing. Where the companies jointly determine the purposes and means of processing, they are joint controllers, but where one company processes data on behalf of another, it is considered a processor (see question 4.1).

Larger group companies with entities outside the EU should consider issuing binding corporate rules as provided in Article 47, which, while having to be approved by the competent supervisory authority, will provide an easier data transfer within the group.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

In case of non-compliance with GDPR stipulations, or in the case of a data breach, the supervisory authority can issue administrative fines of up to 20 million euros, or in the case of an undertaking, up to 4% of the preceding financial year's total worldwide annual turnover of the group to which it belongs, whichever is higher.

10.2 Do individuals have a private right of action? What are the potential remedies?

The following rights exist for data subjects affected by data protection infringements:

(a) Right to lodge a complaint with a supervisory authority;

(b) Right to claim information about one's own personal data according to Article 15;

(c) Right to an effective judicial remedy where a person considers that his/her rights under the GDPR have been infringed as a result of the processing of his/her personal data in non-compliance with the GDPR;

(d) Right to receive compensation from the controller or processor for damage suffered; and

(e) Right to mandate a not-for-profit body, organization or association (which has been properly constituted in accordance with the law of a Member state, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data) to lodge the complaint and exercise the rights referred to above on his/her behalf (in the case of the right to compensation, this applies only where provided for by Member state law).

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of the EU Member states which affect privacy?

Please see the section of each Member state below.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The hottest topic is the ePrivacy Regulation which so far only exists as a draft. The ePrivacy Regulation will regulate the sector of electronic communications. The following electronic communication processes will most likely be affected:

- internet access
- instant messaging services,
- web-based email services,
- internet telephony,
- staff messaging, and
- social media.

It should be mentioned that the ePrivacy Regulation will apply to the processing of both personal and non-personal data and aims to protect the communications data of natural and legal persons.

The changes will affect, in particular, the handling of cookies and the use of electronic means of communication such as e-mail and telephone for advertising purposes. However, as the latest draft has just been rejected by about half the Member states, it does not look like it can come into force in the next one or two years.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in the European Union?

The national data protection authorities of Member states have started issuing rather heavy fines, which means that each controller is strongly advised to take all necessary steps to comply with the requirements of the GDPR and the respective national laws.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

People have become more aware of the value their personal data has. Some Member states have been shaken by data breach scandals and surveillance affairs from companies as well as from foreign states. People are no longer willing to accept this kind of behavior and dare to take back control, eg against major social media companies (see the SCHREMS Law or the "Not Your Business" initiative). At its core, data protection can give a competitive advantage, as customers tend to trust companies that take data protection seriously. People increasingly want to know how the data entrusted to companies is being handled by them.

Also, people have become skeptical towards technological advancements, such as the internet of things, surveillance toys for children, fitness trackers/apps and smart homes and meters, especially because it is unclear how and for what personal data the gadget can and will be used (against data subjects).

12.2 What do you envision the privacy landscape will look like in 5 years?

Hopefully, the current hysteria will have calmed down. First court decisions will have brought a reliable interpretation of current uncertainties in respect of some GDPR stipulations and its interpretation by the authorities. The fines issued within the next five years will provide a more transparent and secure environment as far as personal data is concerned.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Companies will need to stay tuned to developments in such issues as the interpretation and application of the GDPR, which will require not only money and human resources but also changes within the organization of the company.

AUSTRIA

1 PRIVACY LAW

1.1 How is privacy 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 Section 1 of the Austrian Privacy Act and under Article 8 of the Charter of Fundamental Rights of the European Union that is granted under the constitution.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

First of all, the Austrian Data Protection Authority, 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 Article 51of the GDPR.

Secondly, the Austrian courts may rule on privacy matters. They are also competent to award damages for data breaches.

In a recent court decision, it was held that a data subject may only pursue one path in any privacy matter, ie, either seek help from the courts or from the Data Protection Authority.

2 SCOPE

2.1 Which companies are 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; or

(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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 EU, 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 INFORMATION

3.1 How is personal information/personal data defined in Austria?

Personal data has the wide meaning as set forth in Article 4 of the GDPR. See the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

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 him/her with the Data Protection Authority;

(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) use cookies in line with the legal requirements (see question 8.2); and

(j) ask for the data subjects' consent for certain marketing activities (such us promotional emails) etc.

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.

See also the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Austria? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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.

6.2 How are data breaches regulated in Austria? What are the requirements for responding to data breaches?

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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals (data subjects) have the rights specified in the GDPR. See the European Union chapter.

If an individual is denied these rights, he/she can enforce them either through the ordinary courts or by lodging a claim with the Data Protection Authority.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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, his/her email address) is lawful under Article 6 of the GDPR. 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 outweigh those of the individual. If the data subject is a child, this balancing of interests usually is 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, which will be replaced by the ePrivacy Regulation in the near future. Under the Act, the prior consent of the individual is required in almost all cases.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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 question 8.1).

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 the data subject about the tracking and require him/her to disable the same, if the data subject does 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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Again, the rules of the GDPR apply. See the European Union chapter.

Targeting and behavioral advertising usually require the data subject's consent.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Here too, the GDPR applies. See the European Union chapter.

Under the principle of transparency, the data subject has to be informed when data is shared with third parties like Facebook. Furthermore, it is advisable to provide a link to the third-party privacy statement.

Most likely, sharing such data also requires the data subject's consent.

8.5 Are there specific privacy rules governing data brokers?

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.

8.6 How is social media regulated from a privacy perspective?

Again, the GDPR applies. See the European Union chapter.

Otherwise there are no specific rules. Social media platforms are considered as 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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

No.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

There is a wide range of penalties and sanctions, from a warning by the Data Protection Authority to the highest fines under the GDPR (administrative fines up to 20 million EUR, 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 individuals have a private right of action? What are the potential remedies?

Individuals may lodge claims with the courts or the Data Protection Authority.

The courts may award damages and/or prohibit the further processing of data.

The Data Protection Authority may impose fines and also prohibit the further processing of data.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Austria which affect privacy?

The right to privacy is a fundamental right under Austria's constitution.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

No.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Austria?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The GDPR and the massive fines set out therein have triggered more awareness about privacy, both amongst companies and data subjects. This has led, on the one hand, to companies taking an increased number of measures to observe privacy and, on the other hand, to more claims being lodged with the Data Protection Authority by data subjects.

12.2 What do you envision the privacy landscape will look like in 5 years?

After the hype over privacy, which began in 2018 when the GDPR became effective, has settled, privacy will become more commonplace. We will have more clarity on legal privacy issues that are uncertain today, because the number of decisions by data protection authorities and courts will continue to increase.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The challenges will still be the same: implementing effective technical and organisational measures to secure a reasonable level of security and to keep them up-to-date.

Ongoing digitalisation will bring more challenges as digitalisation brings along a huge flow of data, often big data.

BELGIUM

1 PRIVACY LAW

1.1 How is privacy regulated in Belgium?

The Belgian legislative and regulatory landscape to 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 ("*Gegevensbeschermingsautoriteit/ Autorité de Protection de Données*") ("DPA"), by the criminal investigation authorities and by the courts, both directly and upon appeal against decisions of the Belgian data protection authority. 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. See, further, question 3.2.

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 organisations. 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on advertising aspects.

The EU 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 Act of July 30, 2018 on the protection of physical persons towards treatments of personal data ("Privacy Act") is the new 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 are specifically impacting 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) The 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) The Act on Electronic Communications; and

(e) The Act of November 28, 2000 on Cybercrime.

Belgium has no sectoral approach to privacy and personal data protection but the following provide specific rules:

(f) Act of March 21, 2007 on the installation and use of surveillance cameras;

(g) Collective Bargaining Agreement No 68 of June 16, 1998 on camera surveillance of employees;

(h) Collective Bargaining Agreement No 81 of April 26, 2002 on the monitoring of electronic communications of employees;

(i) The Patient Rights Act of August 22, 2002 (specifically on the use of patients' data).

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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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 which are part of Books VI, XII and XIV of the Code of Economic Law. None of the enforcement agencies are self-regulatory.

2 SCOPE

2.1 Which companies are subject to privacy law in Belgium?

See the European Union chapter.

2.2 Does privacy law in Belgium apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy law applies outside the country:

(a) As far as the GDPR is applicable, it applies to companies outside Belgium:

(i) that are established in any EU Member State and that process personal data as a controller or processor, regardless of whether or not the processing takes place in the EU;

(ii) that 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) that are outside the EU, 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 EU of EU residents.

(b) The Belgian Privacy Act applies to controllers and processors that:

(i) process personal data in Belgium (see question 2.1) and

(ii) do not have an establishment in Belgium, but fall within the scope of the GDPR.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Belgium?

Personal data is legally defined in the GDPR Article 4(1) (see the European Union chapter). An identical definition can be found in the Belgian Privacy Act (Articles 2 and 3).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 the age for a child's consent to 13;

(b) A list of three situations in which processing is deemed to be of substantial public interest as an exemption to the prohibition of processing the special categories of personal data (principally racial or ethnic origin, political beliefs, religious or philosophical beliefs). The most relevant one 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 the data controller or processor in relation to the processing of genetic data, biometric data or data concerning health:

(i) indication of which categories of persons have access and explanation of 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

The approach of the Belgian DPA to data protection impact assessments ("DPIA"s) is set out in its February 28, 2018 recommendation, with a Blacklist of processing operations which always require a DPIA. Some of the most relevant operations on the Blacklist 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 services 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 his/her consent or in particular circumstances;

(d) with medical implants where a data breach can compromise physical health;

(e) large-scale processing concerning vulnerable people for purposes other than that 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;

(h) large-scale processing activities by connected devices ("IoT") (eg, generated by devices, smart toys) or systematic processing though the use of automated processing of certain internet data or metadata, viewing, listening and browsing habits, clicking activity or shopping habits.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Belgium? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Belgium? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter and question 1.3 above.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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 the recipient can at any time oppose the further use of his/her electronic contact details for direct marketing purposes) (opt-out basis).

(b) A prior consent of the recipient (opt-in) is also required for marketing by fax or through automated calling machines (Book XII of the Code on Economic Law on the use of emails for advertising purposes).

(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-personalised advertising by post can be stopped through the use of stickers on mailboxes.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

The Act on Electronic Communications implements the 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 EUR 250,000 per day with a maximum fine of EUR 100 million). Other enforcement actions taken by the Belgian DPA have given rise to a EUR 15,000 fine for illegal use of cookies on a website.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

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 (see question 8.1).

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

The maximum penalty for sending marketing communications in breach of the data protection laws is EUR 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 EUR 100 to EUR 30,000 for infringements of the Belgian Privacy Act can be imposed.

10.2 Do individuals have a private right of action? What are the potential remedies?

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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Belgium which affect privacy?

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 Are there any hot topics or laws on the horizon that companies need to know?

The hottest topic is the draft ePrivacy Regulation. 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 cautions around processing personal information/personal data in Belgium?

The Belgian DPA has recently become very active, making recommendations, opinions and decisions on a near-daily basis. One example is a EUR 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 on Planet 49 which determined that effective consent was required for the use of Google Analytics.

Another example is a decision of December 17, 2019 where a EUR 2,000 fine was imposed against a nursing care organisation which failed to act on requests from a data subject to get access to his data and to have his data erased. Several other decisions were made in November 2019, imposing fines for reason of data processing with insufficient legal basis (particularly election mailings to email addresses which had not been collected for this purpose).

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the 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. GDPR is also increasingly being weaponised 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.

BULGARIA

1 PRIVACY LAW

1.1 How is privacy regulated in Bulgaria?

Privacy is regulated on two levels: that of the European Union and that of the Republic 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"), which was last amended with effect from March 1, 2019 to set out derogations and other additional and/or specific data protection rules to the GDPR. The amended PDPA and the Rules on Activities of the Commission for Personal Data Protection and Its Administration (the "CPDP Rules"), effective as of July 30, 2019 also set out the powers and supervision 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") implements the ePrivacy Directive (see the European Union chapter).

National sector-specific laws provide for a few individual sector-specific rules on data protection.

At a secondary legislation level, the CPDP may issue binding rules and instructions regulating the implementation and functioning of legal instruments, such as the technical and organizational measures for personal data protection, set forth in a generic manner in the GDPR or PDPA. Such secondary pieces of legislation have to be in conformity with the relevant primary legal act. Otherwise, they 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The primary legal acts regulating data protection in Bulgaria are the GDPR and PDPA, where the PDPA sets out only the local rules on personal data processing under the opening 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) Employers, in their capacity as data controllers, must adopt special rules and procedures on personal data processing when they have implemented:

(i) an internal system for reporting of violations; and/ or

(ii) control systems of the access, working time and work discipline within their premises.

These must contain information on the scope, obligations and methods for implementation of the respective system in practice and be notified to the employees.

(c) 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 the balancing test criteria which had 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 an implementation of the journalistic exception under Article 85 of the GDPR.

(d) Another specific rule exists with respect to processing personal data for the purposes of creating a photographic or audiovisual work by filming a person in the course of his/her public activity or at a public place. In this case, the PDPA provides that data subjects cannot make use of their privacy-related rights recognized by GDPR, and the regime for data breaches does not apply.

Processing of personal data for marketing purposes is governed by the rules of the GDPR. Limited local provisions also apply with respect to direct marketing via email and telephone (see question 8.1).

There are no state or sector-specific laws and no self-regulatory frameworks applicable to the matter in Bulgaria.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The CPDP is the national supervisory authority. Its powers are provided for in the GDPR and PDPA and the rules and processes for the exercise of such powers are set out in the CPDP Rules. To enforce data protections rules, the CPDP may inspect data controllers and processors, issue and apply mandatory administrative measures and/or impose administrative fines and other sanctions. The CPDP exercises its enforcement powers by issuing decision or other administrative acts which are subject to a judicial review at two 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 the Rules of Operation of the Judiciary Act.

Self-regulatory bodies are not still developed and common in Bulgaria.

2 SCOPE

2.1 Which companies are subject to privacy law in Bulgaria?

See the European Union chapter.

2.2 Does privacy law in Bulgaria apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

In accordance with the scope of application of the GDPR, which is directly applicable in the territory of Bulgaria, privacy law does apply to companies outside Bulgaria. See the European Union chapter.

The PDPA does not contain special rules relating to its scope of application.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In addition to the specific obligations contained in Article 9 of the GDPR, Bulgarian laws provide also 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) Under Bulgarian employment law, the deadline for employers to respond to employee 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

In addition, where data is provided by the data subject without a legal basis, or contrary to the principles under GDPR Article 5, the PDPA obliges controllers and processors, within one month of becoming aware of this, to return the carriers of the data, or, if this is impossible, or requires disproportionate effort, to erase or destroy the unlawfully obtained data. Deletion and destruction of data must be documented.

In light of the principle of storage limitation, the PDPA provides that, in the context of recruitment, the personal data of applicants who have not been offered a job position may be processed no longer than six months after the end of the recruitment process, unless the applicant has given his/her consent for storage of the data for a longer period. Upon expiry of this period, the employer must delete or destroy the stored personal data and return the original documents provided by the data subject. It is worth noting, however, that, in one of its opinions, the CPDP clarified that applicants' data may be stored up to three years, if contained in internal company records created by the employer with respect to the conduct of the application process, on the basis of the legitimate interest of the employer to protect itself against accusations of discriminatory treatment (three years being the statutory deadline for filling a discrimination complaint under the Bulgarian legislation). In such a case, however, the employer must observe the data minimization principle by, eg, pseudonymization of the data.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

The PDPA does not regulate this question.

The CPDP occasionally issues opinions on the allocation of roles regarding the processing of personal data between different companies (eg, in the context of medical assessment of employees done by specialized companies, laboratory medical tests, courier services, etc). 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

In accordance with GDPR Article 35(4), the CPDP has published and announced to the European Data Protection Board ("EDPB") a revised list of the types of processing operations requiring a prior data protection impact assessment. The list contains eight operations which should be taken into account by the 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Bulgaria? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Bulgaria? What are the requirements for responding to data breaches?

See the European Union chapter.

Data breaches related to the processing of personal data for humanitarian purposes by public bodies or humanitarian organizations, as well as processing in cases of disaster within the meaning of the Disaster Protection Act are exempt from the legal regime under the GDPR.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

The Bulgarian legislator has also limited (in accordance with GDPR Article 23) the rights of data subjects under GDPR in cases where the complete exercise of the rights concerned poses a risk to national security, to the prevention, investigation, detection or prosecution of criminal offences, or to other important objectives of general public interest, etc. However, there is no implementing sector-specific regulation effective on the matter as required under GDPR Article 23(2).

According to CPDP interpretations of the applicable data protection laws, the data controller/processor is not entitled to request a notarized power of attorney from a representative of the data subject, where the data subject is not exercising her/his rights personally. Even when handling right to access requests in respect of sensitive data (eg, health-related data), the data controller/processor is not entitled to request a notarized power of attorney and must instead accept a power of attorney in simple written form and/or implement additional, but less burdensome, measures for identification.

The right of a data subject to file a complaint with the CPDP for violation of her/his personal data is statutorily limited to six months after becoming aware of the violation, and, in any event, not more than two years after it was committed. The data subject is not entitled to bring a case 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 yet been issued on the matter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter.

The PDPA specifies that processing data of a data subject below the age of 14 years (ie, a minor), based on consent, including in cases of direct supply of information society services, will be lawful only if the consent is given by the minor's parent or guardian.

In addition, certain direct marketing activities, such as email, telefaxes, 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 regime, 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 them, including via text messages or emails, for the purposes of marketing and advertising its own similar services and/or products, provided that it gives each consumer the option to opt out easily from receiving any future messages for any such purpose. For the purposes of this rule, consumers can be both individual 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 e-mails for the purposes of direct marketing and advertising.

It is worth noticing that the Bulgarian Commission on Consumer Protection keeps a register of the email addresses and telephone numbers of legal entities which have expressly opposed receiving unsolicited commercial communication. Sending unsolicited commercial communication to such contact details of such 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

In Bulgaria, the use of cookies is also regulated by the Law on Electronic Commerce ("LEC"). The LEC 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 LEC have not been tested before the CDPD and the national courts following the GDPR coming into effect. In light of the more recent ECJ case law on the interpretation of the GDPR, we would recommend installing a cookie manager, seeking prior informed consent for each tracking tool.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter, question 8.2.

The CPDP has not issued any guidance on the matter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

No special Bulgarian law rules exist.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

No special Bulgarian law rules exist.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

No special Bulgarian law rules exist.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

The CPDP has already imposed fines:

(a) of BGN 1 million (approx EUR 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; and

(b) of BGN 5.1 million (approx EUR 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 six million persons.

Sanctions for individual ordinary violations of data privacy tend to range between BGN 10,000 and BGN 60,000 (approx EUR 5,000 to EUR 30,000).

Under the Bulgarian Penal Code, some types of information and data security breach qualify as criminal offenses. Those committing such an offense may be subject to imprisonment for a term of between one and eight years and a fine of up to BGN 10,000 (approx EUR 5,000).

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

The right of a data subject to file a complaint with the CPDP for violation of her/his personal data is statutorily limited to six months after becoming aware of the violation, and, in any event, not more than two years after it 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 yet been issued on the matter.

Recently, the Bulgarian Supreme Administrative Court and Supreme Court of Cassation jointly decided that administrative courts should have jurisdiction to hear class action damages claims by data subjects with respect to personal data breaches such as, in the case that was at hand, a massive leak of personal data from the National Revenue Agency.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Bulgaria which affect privacy?

As noted under question 3.2(c), Bulgarian privacy rules and the CPDP are very restrictive in their view on the permissible usage and revealing of PINs of Bulgarian citizens and personal numbers of foreign citizens.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

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 cautions around processing personal information/personal data in Bulgaria?

See the European Union chapter.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

Companies also 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 yet been reviewed and tested in court. In some instances, the adjudications of Bulgarian courts have not been in conformity with relevant ECJ 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.

CROATIA

1 PRIVACY LAW

1.1 How is privacy 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).

The Data Protection Act established a solid framework for the protection of personal data of Croatian residents, which was fully harmonized with the provisions of the EC Data Protection Directive 95/46.

One of country-specific obligations envisaged by the Data Protection Act was the obligation to appoint a data protection officer for all data controllers in Croatia employing 20 or more employees. However, unlike the GDPR, which contains more elaborate criteria regarding the type of processing operations and type of personal data that require the appointment of a data protection officer, as well as about the competences that the data protection officer must possess, the Data Protection Act contained no such additional criteria, and, therefore, in practice, the appointment of a data protection officer was, in most instances, just an administrative requirement rather than an effective instrument for protection of personal data.

The Data Protection Act also imposed a general obligation on data controllers to notify the Croatian Supervisory Authority upfront about their intention to establish filing systems, as well as to register the same with the Croatian Supervisory Authority upon their establishment.

In the application of the Data Protection Act, the Croatian Supervisory Authority was especially active in the field of transfer of personal data outside the territory of Croatia, and a requirement was established for prior approval of appropriate safeguards (principally Standard Data Protection Clauses and Binding Corporate Rules) by the Croatian Supervisory Authority. In the last couple of years before the GDPR started to be applied, any filings with the Croatian Supervisory Authority concerning approvals of such safeguards would trigger the supervision of the applicant by the Croatian Supervisory Authority.

Moreover, in practice, one of the main focuses of the Croatian Supervisory Authority was the processing of personal data through video surveillance; this trend has continued into the GDPR Implementation Act, which contains elaborate provisions relating to the processing of personal data through video surveillance, including country-specific penalties for breach of such provisions (see further question 1.2).

The Croatian Supervisory Authority has established a requirement that consent should always be given by affirmative action, and therefore pre-ticked boxes and similar solutions were not considered as a valid consent. In other words, the Croatian Supervisory Authority had requested affirmative action for giving consent, even before the GDPR entered into force. The GDPR has now made this standard for consent.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The primary source for data protection in the European Union, and thus in Croatia, 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 Member 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. Croatia has done so with the GDPR Implementation Act.

The most important stipulations for the private sector in the GDPR Implementation Act which are based on GDPR opening clauses are the following:

(a) Section 19: 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;

(b) Section 20: The processing of genetic information is forbidden for the purposes of entering into specific agreements in the field of insurance;

(c) Section 22: 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;

(d) Section 23: The processing of biometric data 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;

(e) Section 24: 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;

(f) Section 25: This Section contains definition of processing personal data through video surveillance;

(g) Section 26: The processing of personal data by means of video surveillance may be performed only for a purpose which is necessary and justified for the protection of persons and assets. In this Section, the GDPR Implementation Act also defines which parts of a buildings and space may be subject to video surveillance;

(h) Section 27: This Section contains detailed provisions about the obligation of data controllers or data processors to clearly indicate (by means of a sticker or similar) that a certain object is under video surveillance, and about the information that needs to be included in the respective notice;

(i) Section 28 and 29: Only the responsible person of the data controller, or the person authorized by the responsible person, has the right of access to video surveillance recordings. The data controller and data processor are required to establish an automated log system to

video surveillance recordings. The video surveillance recordings may be kept for a maximum period of 6 months, except in certain exceptional cases (eg, if the same are used as evidence in court or administrative proceedings);

(j) Section 30: Video surveillance of offices is permitted only under conditions envisaged by the GDPR Implementation Act and safety at work regulations (under the latter regulations, video surveillance is permitted primarily for the purpose of protection of persons and assets), as well as under the condition that the employees have been informed about such surveillance in advance. It is not permitted to put up video surveillance in employees' rest rooms, changing rooms and rooms for personal hygiene;

(k) Section 31: This Section contains provisions about the use of video surveillance in apartment buildings, which requires the vote of two thirds of the tenants for such use;

(l) Section 43: This contains provisions about the administrative fee that the Croatian Supervisory Authority may charge for the issuing of opinions to business subjects (eg, law firms, data protection consultants and similar) which have been requested by such subjects as part of their regular business activities;

(m) Sections 44–50: These contain detailed provisions about the procedure for the issuing of administrative fines by the Croatian Supervisory Authority, including provisions regarding the statute of limitation for issuing of the same;

(n) Section 51: This sets out country specific provisions about monetary fines (up to HRK 50,000 approx EUR 6,700) that the Croatian Supervisory Authority can issue in case of breach of the provisions of the GDPR Implementation Act regarding the processing of personal data by video surveillance.

At the beginning of January 2019, the Croatian Supervisory Authority published a consultation draft of the criteria for payment by instalments of administrative fines related to breach of data protection law. The consultation has been completed, and it is expected that the Croatian Supervisory Authority will now proceed with completing and publishing of the criteria.

With respect to processing of personal data for marketing purposes, all relevant stipulations are contained in the GDPR.

Certain aspects of marketing activities, such as the use of electronic communications (email, telephone etc) for the purposes of sending of unsolicited communications are stipulated in the Croatian Act on Electronic Communications ("e-Communications Act") (see question 8.1).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Croatia does not have any 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 which is authorized to monitor, ask questions that need to be answered, perform supervisions, issue corrective measures and administrative fines. It is not possible to appeal against the decisions issued by the Croatian Supervisory Authority, 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 — 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 SCOPE

2.1 Which companies are subject to privacy law in Croatia?

Please see the European Union chapter.

In addition to the GDPR, the Croatian GDPR Implementation Act contains additional provisions regarding the applicability of its provisions on the processing of biometric data. The same provisions 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.

2.2 Does privacy law in Croatia apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy laws apply outside the country. Please see the European Union chapter and question 2.1.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Croatia?

Personal data is legally defined in the GDPR Article 4(1) (please see the European Union chapter).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Please see the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Yes, please see the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Please see the European Union chapter.

In addition, in line with its obligation under Article 35(4), the Croatian Supervisory Authority has published a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment, which is available on its website. The list is largely based on guidelines issued in this regard by the Article 29 WP on this topic.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Croatia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Please see the European Union chapter.

In addition, the Croatian Supervisory Authority has published, on its website, a general description of technical and organizational measures for securing the personal data, which include, inter alia:

(a) Keeping hard copy materials containing personal data in locked lockers or drawers, which should be under the supervision of authorized persons;

(b) Access to personal data by electronic means should be protected by usernames and passwords;

(c) Safety copies (back-up) of records containing personal data should be made by authorized persons;

(d) Employees involved in the processing of personal data should sign confidentiality statements;

(e) Pseudonymization and encryption of personal data should be used, especially in case of special (sensitive) categories of data; and

(f) A system of logs of access to personal data should be established, where applicable.

6.2 How are data breaches regulated in Croatia? What are the requirements for responding to data breaches?

Please see the European Union chapter.

The Croatian Supervisory Authority has published on its website a template of the form for data breach notifications.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Please see the European Union chapter and question 1.3 above.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Please see the European Union chapter.

In addition, The Croatian e-Communications Act contains provisions about use of electronic communications (email, telephone etc.) for the purposes of sending of unsolicited communications.

In line with Article 107 of the e-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 may only be allowed in respect of subscribers or users who have given their prior consent.

A trader, which can be a natural or a legal person, 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.

Consent is not required for telephone calls made to legal persons for the purposes of direct marketing and sale.

HAKOM has also established "Do not call" registries, in which the subscribers can register their telephone numbers in case that do not wish to receive unsolicited communications.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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 ("ECJ") in Case No C-673/17 regarding the standard of consent in relation to use of cookie technology. Namely, HAKOM considers 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 already checked off, 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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Please see the European Union chapter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Please see the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

Please see the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

Please see the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Please see the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Please see the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Please see the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Please see the European Union chapter.

In addition, Croatia has prescribed monetary (administrative) fines (up to HRK 50,000, approx EUR 6,700) that the Croatian Supervisory Authority can issue in case of breach of the provisions of the Croatian GDPR Implementation Act regarding the processing of personal data by video surveillance.

10.2 Do individuals have a private right of action? What are the potential remedies?

Please see the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Croatia which affect privacy?

There are no such rules to the best of our knowledge.

Nevertheless, as stated earlier (see questions 1.1 and 1.2), in practice, one of the main focuses of the Croatian Supervisory Authority has always been the processing of personal data through video surveillance: this trend has continued in the GDPR Implementation Act, which contains elaborate provisions relating to the processing of personal data through video surveillance including country-specific penalties for breach of such provisions.

It is also worth mentioning that the Croatian Supervisory Authority has, so far, been more focused on educating with respect to the GDPR, and less on supervisions. Moreover, to the best of our knowledge, no significant administrative fines have yet been issued. However, we expect that trend to change in the future, and that the Croatian Supervisory Authority will shift its focus to its correctional function.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

We are all awaiting the ePrivacy Regulation.

In addition, and as stated earlier (see question 1.2), the Croatian Supervisory Authority is currently in the process of setting criteria for payment by instalments of administrative fines related to breach of data protection law, and these criteria should be formally adopted soon.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Croatia?

Other than aforementioned, no.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Please see the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

Please see the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Please see the European Union chapter.

CYPRUS

1 PRIVACY LAW

1.1 How is privacy 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, GDPR is directly enforceable and applicable across the EU Member States.

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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

As mentioned above, the GDPR is the primary source of legislation on privacy.

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 clauses, which allow room to EU Member States 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:

(a) Under Article 9 the processing of genetic and biometric data for purposes of health and life insurance is prohibited, except where the data subject gives his consent.

(b) Article 33 constitutes certain infringements of Privacy Law rights as criminal offenses, and sets out penalties for these (see question 10.1). In particular:

  (i) 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 his/her tasks, particularly those relating to the cooperation with the Commissioner; or

  (ii) when a controller does not notify the Commissioner of a personal data breach, or does not carry out an impact assessment.

Further Cyprus has enacted Law 44(I)/2019 (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 one of the other main sources 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.

In addition to the above, 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.

Finally, private life and respect for the secrecy of correspondence is a fundamental right in Cyprus embedded in its Constitution through Articles 15 and 17. These provisions are now to be read in light of the GDPR provisions.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Cyprus does not have any self-regulatory bodies which enforce privacy law.

The GDPR and other privacy laws are enforced by the National Competent Authority which is the Office of the Commissioner for Personal Data Protection ("Commissioner'"). The Commissioner 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.

2 SCOPE

2.1 Which companies are subject to privacy law in Cyprus?

See the European Union chapter.

2.2 Does privacy law in Cyprus apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy law applies to companies outside the country see the European Union chapter.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Cyprus?

Personal data is legally defined in the GDPR Article 4(1) (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 (Article 2 of both Laws).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Apart from the specific obligations regarding information under Article 9 of 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Cyprus? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Cyprus? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter and see question 1.3 above.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

There are some direct marketing activities, such as emails, telefaxes, text messages and phone calls, which are subject to Part 14 of Law 112(I)/2004, and are, as a general rule, only permissible on the basis of a valid and informed prior consent that has been given by the subscribers/users regarding the specific means of direct marketing (Article 106).

Regarding the cookie policy of websites, Article 99(5) of Law 112(I)/2004 is relevant, as well as Article 5(3) of EU Directive 2002/58/EC which was amended by Directive 2009/136/EC whereby the storing of cookies requires express consent.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter and see question 8.1 above.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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 Article 17 of 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, Article 18 of 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) Article 38 of 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 as provided for in Article 39 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter in respect to the GDPR.

Apart from the GDPR, Article 33 of Law 125(I)/2018 renders several breaches of privacy law as criminal offences. If a person is convicted of committing any of the offenses that are referred in the Article, 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 Euros. Further, according to Article 54 of Law 44(I)/2019, the Commissioner has the power to impose on a controller an administrative fine in case of infringement of up to100,000 Euros.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

Apart from making complaints to the Commissioner pursuant to Article 50 of Law 44(I)/2019, 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.

Any person who has suffered material or non-material damage as a result of improper processing or any act by the controller or other competent authority in breach of Law 44(I)/2019 is entitled to compensation.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Cyprus which affect privacy?

See the European Union chapter.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The judgment of the EU Court of Justice in the Planet46 GmbH case (Case No C-673/17) (as to which see the European Union chapter, question 8.2) will change the status quo regarding the cookie policy and consent, even though the definition of "freely given" consent remains unclear and ambiguous. This decision is of great importance in light of the issues surrounding the use of personal data on the internet.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Cyprus?

See the European Union chapter.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/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 do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the 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 now been transformed into a more precise and certain approach by the EU Member States. However, given that the GDPR has only been enacted recently, the case law remains blurred, whilst privacy is more vulnerable than ever before. The EU Court of Justice has to promote the certainty and uniformity of the system, as there is a need to reduce the information asymmetries which still exist. As a result, the EU regulators have to place under the microscope a feasibly high level of data protection whilst concurrently giving individuals direct access to justice through a private right of action.

CZECH REPUBLIC

1 PRIVACY LAW

1.1 How is privacy 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 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 ("Czech DPA"); and the recommendations and guidelines of the European Data Protection Board.

The first law specifically regulating personal data protection in the Czech Republic was the Act on Protection of the Personal Data in Information Systems adopted in 1992. This Act generally stipulated the basic rules relating to data privacy and definitions, such as personal data, data subject and information systems. However, there were no sanctions for breaching the provisions of this Act and no supervisory authority to control it.

An important development in the data privacy field in the Czech Republic was the accession to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("ETS 108"), which was first European document regulating personal data transfers, in 2000.

Following the signature of ETS 108, the Act on Personal Data Protection ("APDP"), was adopted in 2000. The APDP introduced sanctions for violation of duties related to personal data protection and processing, and created the first Czech supervisory authority (the DPA). After the accession of the Czech Republic to the European Union, the APDP was fundamentally amended in order to be compliant with European data protection rules. The APDP constituted comprehensive legal regulation of personal data protection and personal data processing. Therefore, the entry of the General Data Protection Regulation ("GDPR") into force in May 2018 did not constitute a major difference to our legal environment. However, as a result of a large media campaign concerning the GDPR and its huge sanctions and new concepts (which were often misinterpreted by media), the data privacy regulation came to the attention of majority of the business companies and entrepreneurs for the first time in 2018.

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 the APDP, which was then completely repealed by the new Act on Personal Data Processing ("NAPDP") adopted in April 2019.

The primary objective of the GDPR is to protect the fundamental rights and freedoms of individuals, with a focus on the right to the protection of personal data. The GDPR adopts all existing data protection and processing principles introduced by the 1995 Data Protection Directive, though it explains and complements them more extensively. The GDPR further develops and strengthens the rights of people affected by processing. In addition to new concepts (such as data protection officers, records or impact assessment), the GDPR also requires data controllers to be significantly more active.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The constitutional basis of personal data protection is stipulated in Articles 7, 10.3 and 13 of the Declaration of the Fundamental Rights and Freedoms of the Czech Republic. These rules are 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 generally regulated by the Czech Civil Code.

Personal data protection is regulated comprehensively by the GDPR and the NAPDP. The GDPR provides for majority of legal obligations. The NAPDP 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. It is therefore important that the GDPR and the NAPDP are read side by side.

The NAPDP 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 defence 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 NAPDP has not used the possibility of amending general GDPR rules in many cases. However, the NAPDP 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 adjust 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.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The Czech Republic does not have any self-regulatory bodies which enforce privacy law.

The obligations stipulated by the GDPR and the NAPDP or other applicable legal regulation are enforced by the Czech DPA and, in cases where the decision of the DPA is appealed, by the Czech courts.

The Czech 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 Czech DPA has a role in supervising electronic communications, as provided by the Electronic Communications Act. Supervision of bulk commercial communication is regulated by the Act on Selected Services of the Information Society ("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 Czech 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 Czech 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.

2 SCOPE

2.1 Which companies are subject to privacy law in the Czech Republic?

See the European Union chapter.

2.2 Does privacy law in the Czech Republic apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Privacy law applies also outside the Czech Republic.

See the European Union chapter.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in the Czech Republic?

See the European Union chapter.

Whilst the definition of "personal data" stipulated in the GDPR has not changed from that in the APDP, the interpretation and the scope of "personal data" in the Czech Republic is more extensive in practice due to case law (see, eg, SDEU (C-434/16) case Nowak).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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) is essential to determine the risks related to liability in case of a data security breach or other violations under the GDPR.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

In addition, it is explicitly stipulated in the NAPDP 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.

In the SSIS, the responsibility of certain services providers is also stipulated:

(a) the provider of a service consisting of the transmission of information provided by the user via electronic communications network, or intermediation of access to electronic communications networks for the purpose of transmission of information (including automatic temporary storage of transmitted information) is responsible for the content of transmitted information only if the provider:

  (i) initiates the transmission by himself,

  (ii) chooses the user of transmitted information, or

  (iii) chooses or modifies the content of transmitted information;

(b) the provider of a service consisting of the transmission of information provided by a user is responsible for the content of information automatically temporarily stored only if the provider:

  (i) modifies the content of information,

(ii) fails to meet the conditions of access to the information,

(iii) fails to comply with rules on updating of information generally accepted and used in the respective industry,

(iv) exceeds permitted use of technology generally accepted and used in the respective industry with the objective of gaining data on use of information, or

(v) fails to immediately take measures to remove the information stored by him or to prevent access to such information if he finds out that the information was removed from the network at the initial place of transmission, or the access to such information was prevented, or the court ordered withdrawal or prevention of access to such information;

(c) the provider of a service consisting of the storage of data provided by a user is responsible for the content of information stored on demand of the user only if the provider:

(i) knows, with regard to the scope of his activities and circumstances and the nature of the case, that the content of stored information or user's conduct are unlawful, or

(ii) can be shown to have discovered the unlawful nature of content of stored information or unlawful user's conduct and failed to make all steps which may be reasonably requested for him to make in order to remove or prevent access to such information.

The above providers 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in the Czech Republic? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter for the minimum standard for securing data.

The NAPDP stipulates specific standards and rules for securing data which apply to personal data processing for the purpose of ensuring defence and security interests of the Czech Republic.

Further specific standards for data security are stipulated in the Act on Cyber Security.

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 the company with guidance in this matter.

6.2 How are data breaches regulated in the Czech Republic? What are the requirements for responding to data breaches?

See the European Union chapter for basic regulation following from the GDPR.

The DPA usually proceeds in line with the guidelines of the European Data Protection Board (formerly known as Working Party 29), which endorsed the former WP 29 Guidelines on Personal Data Breach Notification under Regulation 2016/679.

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, which leads 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 high 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 subject 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, especially if there is a high risk that it will affect their personal rights.

There are exemptions from this obligation where:

(a) the controller has 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

In addition, electronically disseminated commercial communications are specifically governed under Czech law. One may only use an electronic contact (eg, email) for the purpose of disseminating commercial communications electronically if the users have granted their prior consent.

However, if a natural or legal person obtains electronic contact details from its customer in relation to selling products or services to him, such person may use these electronic contact details for the purpose of disseminating commercial communications related to its own similar products or services. This is possible on condition that the customer has a clear opportunity to easily withdraw his consent to such use of his 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:

(a) is clearly labelled as commercial communication,

(b) does not hide or conceal the identity of the sender on whose behalf the communication takes place, and

(c) contains a valid address to which the addressee can directly and effectively send the information that he does not wish commercial information to be sent to him by the sender anymore.

The agenda of (unsolicited) commercial communications is governed by the DPA and the DAPA regularly undertakes inspections in this field.

The DPA issued a brief opinion on electronic marketing communication in 2018, in which it recommended that entrepreneurs always use checkboxes in electronic advertising for electronic marketing communication, not for consent (as consent is not necessary and should not be the legal ground of processing), but to allow the user the chance to refuse to receive the commercial communication before the entrepreneur starts to send it.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

In addition to the EU regulation, there is also national legislation stipulating certain provisions on the use of tracking technologies. The Act on Electronic Communications 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 same Act 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 terminal equipment of participants or users is obliged to provably inform such participants or users in advance on the extent and purpose of their processing and is also obliged to offer them the opportunity to decline such processing. This does not apply only in case of technical storage or access exclusively for the purpose of transmitting messages via electronic communications network, or where necessary to provide the information society service explicitly demanded by the participant or the user.

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 him based on the Act, 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 his device resulting from a cyber security incident.

In relation to the GDPR, the DPA has also published a draft recommendation for the processing of cookies and other tracking technologies. In this recommendation, the DPA states that the new ePrivacy

Regulation has not yet been approved and thus it is necessary to follow national legislation, along with certain rules for the processing of personal data stipulated in the GDPR.

The DPA stipulates in its recommendation that a user's consent is necessary for the use of cookies. In this context, the DPA stipulates that a particular setting of the web browser made by the user, ie, whether the browser should allow a website to store cookies in the terminal equipment, may be considered as a consent to the processing of personal data. For the processing of data obtained based on such cookies, it is necessary to establish a suitable legal ground under Article 6(1) of the GDPR. If the legal ground is consent, further criteria and rules are stipulated in the GDPR. Consent is interpreted in relation to the purpose, means and manner of processing of personal data, not in relation to the product or web application; once consent has been granted, eg, for third party cookies, there is no need to further specify a particular search engine or news server.

The recommendation is not applicable to cookies necessary for ensuring the operation of websites and internet services, where obtaining the user's consent is not necessary. We believe that this recommendation will be amended based on recent case law and the ePrivacy Regulation.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter and question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

In addition, at the beginning of 2020, the DPA issued guidelines on the obligation of controllers to perform data protection impact assessments ("DPIA"s), with a list of activities that are not subject to DPIAs.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

In addition to what is mentioned in the European Union chapter, under the NAPDP, the state authorities are not subject to the fines stipulated in the GDPR. Moreover, the NAPDP stipulates a specific fine of up to EUR 200,000 for breaching the ban on processing of personal data imposed by specific Czech legal regulation.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of the Czech Republic which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The hottest topic is the draft ePrivacy Regulation as stipulated in detail in the European Union chapter.

We also consider European and Czech legal regulation of cyber security to be a hot topic.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in the Czech Republic?

There are no GDPR-related court cases, and only a few resolutions of the DPA on breaches of the GDPR. This is because the NAPDP has been effective only as from April 24, 2019, and, before then, the DPA only issued warnings and recommendations. Nevertheless, we believe that the approach of the DPA will be similar, both in terms of sanctions and assessment of specific data privacy related situations, to its approach under the previous, pre-GDPR, regulation, whereby it did not fine companies for mistakes in data privacy documentation or processes, or imposed only very low fines (mostly between EUR 100 and EUR 1,000); the highest fine imposed for breach of the APDP in the field of data protection was EUR 150,000 (for the loss of personal data of 1.2 million clients of the processor in telecommunications) and EUR 180,000 in the field of unsolicited commercial communications.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

Companies undertaking business in the Czech Republic should be more active in the data privacy field, and ensure that their business and internal activities are compliant with data privacy law. GDPR audits and data protection impact assessments should become a regular feature of common business practice.

We also consider the processing of biometric data (in particular in internal administration and processes of companies), the processing of personal data of children under 15 years of age on the internet, and general regulation of advertising on the internet to be future challenges in this field.

DENMARK

1 PRIVACY LAW

1.1 How is privacy regulated in Denmark?

Privacy is regulated by both applicable Danish law and European law. The laws 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.

By the 1960s and 1970s, it had become apparent in Denmark that neither the Danish nor the international regulation of privacy was sufficient. The European Convention on Human Rights had a very broad protection of privacy in its Article 8, but could not grant the necessary protection needed with the arrival of electronic information technology. Moreover, the Danish Constitution only protects secrecy of communication, and does not grant sufficient protection of personal data. This lack of data protection led to the first regulation of personal data in 1978 in the form of the Registry Laws. These were two laws that regulated registries containing personal data for the public administrations and the private sector respectively.

The regulation of personal data in Denmark then followed the developments in Europe, with the next major development coming with the Data Protection Directive in 1995. It took Denmark unusually long, five years in fact, to implement national law on the basis of the Data Protection Directive. The Directive was implemented with the Personal Data Act. The Directive, together with the Personal Data Act, constituted the regulation of privacy in Denmark until the GDPR entered into force in 2018.

With the GDPR, the previous Personal Data Act was abolished and replaced by a new law, the Data Protection Act, which specifically regulates the areas in which the GDPR leaves openings for the Member States to regulate themselves. In the same way that the GDPR is more an evolution than a revolution of the Directive before it, so too is the Danish Data Protection Act only an evolution of the previous Danish Personal Data Act.

The GDPR and the Danish Data Protection Act together regulate privacy in Denmark today. The Danish Data Protection Act refers to the GDPR, in that it supplements and implements the GDPR in Denmark. In areas that are regulated by both the GDPR and the Data Protection Act, it is the GDPR's regulation and principles that apply.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The GDPR and the Danish Data Protection Act are the two key laws regulating privacy in Denmark. As the GDPR is an EU Regulation, it is directly applicably in all member states, including Denmark.

For the GDPR, please see the European Union chapter.

The Danish 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 Danish Data Protection Act:

(a) regulates when 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 Danish 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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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.

2 SCOPE

2.1 Which companies are subject to privacy law in Denmark?

Please see the European Union chapter.

The Danish Data Protection Act applies to the processing of personal data carried out on behalf of a data processor or data controller that is established in Denmark, regardless of whether the processing is done inside the European Union.

2.2 Does privacy law in Denmark apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy law applies to companies outside the country:

As far as the GDPR is applicable, it applies to companies outside Denmark.

The Danish Data Protection Act applies to companies outside of Denmark if the data processing is carried out on behalf of a data processor or data controller that is established in Denmark.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Denmark?

The definition of "personal data" in Denmark is the same as in the GDPR article 4(1). Please see the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Please see the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Please see the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Please see the European Union chapter.

Both the Danish Data Protection Act and the Danish Marketing Act specifically dictate that sending direct marketing to consumers requires the specific, express consent of the consumer.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Denmark? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Please see the European Union chapter.

Data breaches must be addressed to the DDPA.

6.2 How are data breaches regulated in Denmark? What are the requirements for responding to data breaches?

Please see the European Union chapter.

Data breach reports must be addressed to the DDPA.

Reporting of data breaches in Denmark can be omitted if there are substantial private or public interests against it. Furthermore, reports of data breaches are not required if this will make criminal investigations more difficult.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Please see the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Please see the European Union chapter in general.

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 Danish 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 Danish Marking 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 that they have received from a consumer in connection with a sale, even without a consent. 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Please see the European Union chapter in general.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Please see the European Union chapter in general.

It is still up for debate whether behavioural advertising, such as ads on social media platforms or banner ads, are direct marketing that requires consent under Danish law. Consent is usually required and therefore advisable, since it would be difficult to claim legitimate interests as a lawful basis for data processing.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Please see the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

Please see the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

Please see the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Please see the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Please see the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Please see the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Please see the European Union chapter.

In egregious cases, sanctions can be imposed in the form of prison sentences on natural persons. This was also the case under the EC Data Protection Directive, but was never used. It is unlikely that it will be used under the GDPR, but such sanctions are still present in case of very egregious actions by natural persons acting on behalf of companies.

Sanctions have been given a statutory limitation of 5 years for breaches both of the GDPR and of the Danish Data Protection Act.

10.2 Do individuals have a private right of action? What are the potential remedies?

Please see the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Denmark which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

As with the rest of Europe, the forthcoming ePrivacy Regulation is the big hot topic.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Denmark?

The DDPA regularly issues and updates its guidelines. It also updates and informs about its practice. It is generally advisable to be aware of how the DDPA interprets the privacy laws of Denmark and any changes to its interpretation.

This last year has seen the DDPA report two companies, where it recommended fines of over DKK 1 million to each of them. The size of the fines is rather large in a Danish context, but they are less so when compared to the larger fines seen in other European countries to date.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The need for an EU Regulation on data protection arose in part because of the increasing use of technology and the more complex nature of technology itself. This has led to an ever-increasing amount of personal data being processed by companies. Personal information has many forms today. One could, for example, look at the way Internet of Things ("IoT") devices have reached inside our homes and continue to do so more and more. The spread of IoT devices will bring many challenges from a privacy perspective, as data processing will only get more complicated and more vulnerable. Both data subjects and companies must be aware of the data processing principles in the GDPR going forward, when our lives will be more connected to technology, because the technology will only get more complicated and more connected.

12.2 What do you envision the privacy landscape will look like in 5 years?

The hysteria regarding the practical requirements of the GDPR will most likely die out and the processes needed for complying with the GDPR will be normalized. Data protection and privacy will still be important and may even gain greater importance around the world. Having said that, it does seem unlikely that there will not be any difficulty in adhering to the GDPR in 5 years. Companies still have a long road ahead in changing their everyday processes so that privacy is respected in the way the GDPR demands.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The uncertain nature of the fines and how the courts will interpret the GDPR will be a challenge for companies. It is therefore advised that companies make sure that they are in compliance with the GDPR. Companies also continually have to make sure they are adhering to the privacy regulation, especially when new technologies arise and spread.

FINLAND

1 PRIVACY LAW

1.1 How is privacy regulated in Finland?

There is a constitutional right to privacy under Finnish law. Section 10 of the Constitution of Finland (731/1999, as amended) states that 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 below.)

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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

In addition to the GDPR, the DPA supplements and specifies certain parts of the GDPR. The main national additions or specifications to the requirements of the GDPR include the following:

(a) 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.

(b) Specifications regarding administrative fines: Administrative fines may not be imposed on public authorities or bodies in Finland.

(c) 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 named "data protection offence", applicable only to natural persons, has been introduced.

(d) 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.

(e) Supervisory Authority: The competent local supervisory authority will continue to be the Finnish Data Protection Ombudsman. (The Finnish Transport and Communications Agency ("Traficom") will remain the supervisory authority in e-privacy matters.)

Finland's data protection laws also include separate provisions on the processing of employees' personal data, which are covered by 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,

eg, 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.

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, eg, provisions relating to the use of cookies (see, further, question 8.2), 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 8.1.

The Criminal Code of Finland contains several criminal sanctions relating to privacy matters, such as the data protection offence. In connection with the reform of the Finnish PDA, the Finnish Criminal Code's provisions on privacy were also repealed in order to avoid criminal sanctions overlapping with administrative ones.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

In Finland, the Data Protection Ombudsman (tietosuojavaltuutettu) is the local supervisory authority which supervises the 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 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy law applies outside the country. 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 the local office in Finland or where the employment contract is governed by Finnish law.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Finland?

Personal data is legally defined in the GDPR Article 4(1) (see the European Union chapter). No separate definition is contained in the DPA.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In addition, Sections 6 and 7 of the DPA provide exceptions where Article 9(1) of 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 Section 6 of the DPA, such as pseudonymisation, encryption and appointing a data protection officer.

Consent to process 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 to 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 employee him-/herself, 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Finland? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Finland? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

The requirements for direct electronic marketing are set forth in Chapter 24 of the Act on Electronic Communications Services, which sets 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 to easily, and at no charge, prohibit direct marketing.

(c) Where a service provider has obtained the 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 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 his/her position in the organization.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

In addition, cookies are regulated in national legislation under Section 205 of 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 his/her consent thereto and the service provider gives the user comprehensible and complete information on the purposes of saving or using such data. 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.

In Finland, the ePrivacy Directive (2002/58/EC) has been interpreted to allow the user to consent to the storage of cookies, eg, through browser or other application settings. The storage and use of data is allowed only to the extent required for the service, and it may not limit the protection of privacy any more than is necessary.

It should be noted that the Court of Justice of the European Union ("CJEU") has recently ruled on consent requirements for cookies (Case C-673/17, Planet49). According to the judgement, the website operators aiming to store cookies on a user's device must obtain active and specific consent. Accordingly, the CJEU ruled that any opt-out consent, by way of pre-ticked checkbox is insufficient for the storage of cookies. However, as the ePrivacy Regulation is still being drafted by the European Union, the conditions for cookie consents are still interpreted in accordance with the national laws on cookies. Traficom, which is the competent national authority, has updated its guidelines on cookies after the CJEU ruling. However, the revised guidelines still reflect the broad interpretation of consent to cookie tracking, since the guidelines note that cookie consent may be given through, eg, browser settings.

The answers above, as well as the current national interpretation, may need to be revised in the near future as a result of the upcoming ePrivacy reform. Once the EU ePrivacy Regulation has entered into force, the Regulation will be directly applicable across the European Union, harmonizing the cookie consent question on the EU markets.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter, and questions 8.1 and 8.2 above.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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. The 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 Section 24 of 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 context of employment, the employer will be sentenced to a fine, unless a more severe penalty is provided in another Act.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Finland which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

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 cautions around processing personal information/personal data in Finland?

According to the DPA, decisions of the Data Protection Ombudsman (as well as the Deputy Data Protection Ombudsmen) and decisions on administrative fines may be appealed against by filing an appeal in an Administrative Court. It should be noted that a decision may state that the decision is enforceable notwithstanding appeal. In practice, this means that the (possibly unfavorable) decision becomes effective immediately. However, obtaining a court order prohibiting enforcement of such decision may be possible in certain circumstances.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

FRANCE

1 PRIVACY LAW

1.1 How is privacy 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. The 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).

The CNIL's guidelines and opinions are not binding the courts but are usually taken into account by the judges.

Privacy has been regulated in France since the law dated January 6, 1978 ("Data Protection Law"). It was amended on June 20, 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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 the majority of privacy regulation.

The Data Protection Law aims at implementing the opening clauses; the main rules aiming 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, in particular 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 have 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 the CNIL in certain instances, in particular, processing for research purposes when the processing does not meet the guidelines issued by the CNIL;

(d) a child must be at least 15 years old to give a valid consent for the processing of his/her personal data (the GDPR sets the age at 16 years, but EU Members States are allowed to provide for a lower age);

(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, in particular 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, defence or public security.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

France does not have any self-regulatory body which can enforce privacy law.

The GDPR and the Data Protection Law is enforced by the CNIL, the French supervisory authority which has the following powers :

(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 the 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 in the event that a lawsuit is brought by a data subject claiming that his/her rights have been violated and claiming a civil or criminal liability (depending on the violation) from the data controller or processor.

2 SCOPE

2.1 Which companies are subject to privacy law in France?

See the European Union chapter.

In addition to the scope of the GDPR, French 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy law applies outside the country:

(a) As far as the GDPR is applicable, it applies to 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.

The Data Protection Law no longer imposes the requirement that the data controller, which is not established in France (or in another EU Member State), must appoint a representative located in France.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in France?

The Data Protection Law makes a reference to the GDPR for the definition of personal information/personal data. See the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In addition to specific obligation 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 does not lead to the re-identification of the individual concerned (see question 1.2(b)).

The controller or processor must take appropriate and specific measures to safeguard the interests of the data subject.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in France? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in France? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter and question 1.3 above.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

In addition, certain direct marketing activities, such as marketing by email, telefaxes, SMS and automatic calling, are subject (as a general rule for B2C communications) to the prior informed consent of the recipient (ie, opt-in; no pre-ticking of the boxes) under the Electronic Communication and Postal Service Code. There are exceptions to the opt-in rule when the recipient is already a customer and the purpose of the marketing communications relates to products or services similar to those previously purchased by the customer (in such a case, the opt-out principle applies: the recipient can refuse any further communication when he/she receives the marketing communications).

The CNIL confirmed, in a public release, that the GDPR does not affect the above rules (so that a specific consent must be obtained for the sending of such communications).

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

On July 4, 2019, the CNIL issued guidelines pertaining to the use of tracking technologies such as cookies. The former version of these Guidelines was no longer compliant with the GDPR (under the former guidelines, the fact that an internet user continues browsing was deemed a valid consent). The current version of the CNIL's Guidelines is now in line with the GDPR concerning the need for the explicit consent of the internet user, as set forth by the GDPR.

These Guidelines will be supplemented at the beginning of 2020 by a Recommendation in order to enlighten operators on practical methods to obtain the internet user's consent (see question 8.3).

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter.

On January 14, 2020, the CNIL launched a public consultation, open (to companies acting in this field of activity, and to the public) until February 25, 2020, as part of its draft Recommendation (see question 8.2 above) on targeted advertising.

According to the CNIL, the purpose of this Recommendation (soft law) is to guide the professionals concerned in their process of compliance. Thus, it will describe possible practical methods to obtain consent in accordance with the applicable rules, and contain concrete examples of user interface, and describe good practices allowing companies to go above and beyond legal requirements.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

On April 27, 2017, the CNIL sanctioned Facebook Inc and Facebook Ireland for the violation of the Data Protection Law and ordered them to pay a fine of 150,000 Euros. During its investigations, the CNIL noted, in particular, that cookies were stored on the devices of users who were not registered with Facebook (the cookies allowed Facebook to track the browsing of a user and to collect such user's browsing data if the user visited a third party's website containing a social media tool, such as a "like" button).

According to the CNIL, the data were not collected and processed in a fair way, due to the absence of sufficiently clear and precise information on the collection of data carried out, and because the cookie made it possible to carry out a detailed monitoring of the browsing of all internet users (whether or not registered on Facebook's social network).

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 his/her 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 Euros (when the infringer is an individual) or 1.5 million Euros (when the infringer is a legal entity).

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter and question 10.1 above.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of France which affect privacy?

Section 9 of 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".

The scope of Section 9 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 Are there any hot topics or laws on the horizon that companies need to know?

The hottest topic is the draft ePrivacy Regulation. 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 cautions around processing personal information/personal data in France?

On January 21, 2019, the CNIL, in application of the GDPR, imposed a penalty of 50 million Euros on Google LLC, for lack of transparency, unsatisfactory information, and lack of valid consent for the personalization of advertisement.

According to the CNIL, the users' consent was not sufficiently informed. The information on these treatments, diluted between several documents, did not allow the user to become aware of their scope. For example, in the section dedicated to "Personalization of ads", it was not possible to take note of the plurality of services, sites, applications involved in these treatments (Google search, You tube, Google home, Google maps, Playstore, Google photo etc) and, therefore, the volume of data processed and combined.

In addition, the CNIL found that the consent obtained was not "specific" and "unequivocal".

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

The hottest topic is the draft ePrivacy Regulation and the interpretation and implementation of the CNIL's Guidelines pertaining to the use of cookies, in particular for advertising purposes (see questions 8.2 and 8.3 above).

GERMANY

1 PRIVACY LAW

1.1 How is privacy 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 is now, therefore, 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.

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.

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. Other important sources that impact data protection and contain important data protection rules are: the Federal Telecommunications Act ("TKG") and the Federal Telemedia Act ("TMG"), as well as the ePrivacy Directive, which had a certain impact on these Acts.

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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on advertising aspects.

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 European Member states and does not need to be implemented by the individual EU Member 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) Section 22: For certain purposes relating to social security, healthcare and the public interest, private bodies are allowed to process special categories of personal data (modifying GDPR Article 9). The procession of personal data of employees has additional provisions (Section 26).

(b) Sections 29, 32, 33: Exceptions to the requirements of GDPR Articles 13–15 apply in certain cases: eg, where confidentiality obligations exist or if the information would undermine the enforcement of civil claims.

(c) Section 35: Further exceptions are made to the data subject's right to cancellation of data under GDPR Article 17.

(d) Section 38: More detail is provided as to when a DPO is needed under GDPR Article 37 (see question 5.1).

(e) Section 26: A comprehensive regulation is provided for the protection of employee data, modifying GDPR Article 88 .

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") (see question 8.1).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Germany does not have any self-regulatory bodies which enforce privacy law.

The GDPR, the BDSG and other laws protecting personal data are enforced by the supervisory authorities (Aufsichtsbehörden) as well as the competent administrative authority. They can monitor, ask questions that need to be answered and issue orders and fines in case of violations of the data protection laws.

2 SCOPE

2.1 Which companies are 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 any establishment of the controller or processor in Germany or in the EU, or the data subject being in the EU (Section 1(4)).

2.2 Does privacy law in Germany apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 (see question. 2.1),

(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 (Section 1(4)).

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Germany?

Personal data is legally defined in the GDPR Article 4(1) (see the European Union chapter). An identical definition is contained in BDSG Section 46.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In addition to the specific obligations contained in the GDPR Article 9, BDSG Section 22(1) permits private bodies to process special categories of personal data for certain purposes, eg if:

(a) processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations; or

(b) processing is necessary 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 has to take appropriate and specific measures to safeguard the interests of the data subject.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

The general requirement in GDPR Article 37 to designate a Data Protection Officer ("DPO") is modified so that a DPO is required only if the controller or processor constantly employs, as a general rule, at least 20 persons dealing with the automated processing of personal data. However, if the processing by a controller or processor is subject to a data protection impact assessment, or if they commercially process personal data for the purpose of transfer, anonymized transfer, or for purposes of market or opinion research, they must designate a data protection officer regardless of the number of persons employed in processing (BDSG Section 38).

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Germany? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter. The German national Data Protection Conference (of the Federal Government and the Federal States) ("DSK"), as well as the various state authorities, issue guidelines for aspects of the GDPR, which can be found online on the respective authorities' website. However, the courts are not bound by these guidelines which only reflect the interpretation of the GDPR by the respective authority. It remains to be seen whether the courts will confirm or replace such guidelines with their own interpretation.

6.2 How are data breaches regulated in Germany? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

In addition, certain direct marketing activities, such as email, telefaxes, text messages and phone calls are subject to UWG Section 7, 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.

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.

No pre-checked boxes are allowed. If consent is contained in other clauses (eg, of standard terms) it must be highlighted.

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 he/she would like to receive information by e-mail 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 recent decision of the Austrian data protection authority indicates that not using the double opt-in procedure when requesting a consent could constitute a violation of GDPR Article 32, which requires the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter question 8.2.

Consent is usually necessary, especially for services where the collected data is transferred to a third-party provider that then processes this data for its own purposes (eg for providing user-specific advertisement on other websites), although the DSK does not currently rule out the possibility of basing web tracking on the legitimate interest of the website operator However, the balancing of interests within the framework of Article 6(1)(f) of the GDPR requires a substantial examination of the interests, fundamental rights and fundamental freedoms of the parties involved, the scope of the data processing, as well as the predictability for the user, and must be related to the specific individual case. Inadequate or general findings that data processing is permissible pursuant to Article 6(1)(f) do not fulfil the legal requirements.

In the light of the uncertainty as to the right test, and the risk of high fines in case of non-compliance, it is advisable to install a cookie manager seeking informed consent for each tracking tool. If external tools are used, data controllers and third-party tracking tool providers need to sign (joint) controllership agreements.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter. A court decision confirmed the consent requirement for customer matching like Facebook Custom Audiences. Facebook would not act as a mere processor for the advertiser but is a third party. This would also require a joint controllership agreement (which Facebook currently does not offer) and a respective clause in the privacy policy.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

With regard to Facebook fanpages and social plug-ins, please note the following:

In June 2018, the ECJ (Case No C-210/16) decided that fanpage operators in the EU, together with Facebook Ireland, should be regarded as data controllers. Facebook responded by offering such an agreement. However, according to a communication of the DSK in April 2019, this agreement is not sufficient to comply with the requirements of Article 26 of the GDPR, because Facebook wants to have sole decision-making power over the data processing. In addition, the DSK is of the opinion that the agreement is not sufficiently transparent and concrete. Thus, according to the DSK, GDPR-compliant operation of Facebook fanpages is currently not possible. A recent decision of the Federal Administrative Court confirmed that the authorities can order the shutdown of fanpages in cases where they do not comply with the GDPR.

When incorporating a social plug-in, eg, Facebook's "like" button, care should also be taken to ensure that the consent allowing data processing (GDPR Article 6(1)(a)) is given *prior* to data processing. Technically, this can be implemented, eg, with the so-called "two-click" solution. The "two-click"

solution means that the user, before activating the plug-in with the first click, will be informed, so that a valid consent can be granted. No data must be processed before this activation. Only after this first click the user can click the social plug-in (eg, the "like" button).

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter. Whether cease-and-desist claims can be brought by individuals against controllers that violate the individual's rights is currently unclear. Court decisions are not unitary and so far there has been no Supreme Court decision in this respect. The same applies for cease-and-desist claims by competitors based on the UWG.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Germany which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The hottest topic is the draft ePrivacy Regulation. See the European Union chapter. Other hot topics are the assessment of compliance regarding fanpages and the approach the authorities will take concerning tracking tools/cookies.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Germany?

After an initial reluctance to issue fines, the data protection authorities have now started to do so. Fines issued so far vary between 10,000 euros and 14,500,000 euros. Especially fine-sensitive are violations of the information requirements resulting from data breaches; but fines have also been issued for insufficient technical and organisational measures to ensure information security, non-appointment of a data processing officer and general lack of a legal basis for data processing. Usually the immediate cooperation of the controller with the authority will help to reduce the amount of the fine.

In addition, the DSK has recently issued a model to calculate fines in cases of violation of the GDPR. When applying the model, the suggested amounts are much higher than the previously issued fines. The model serves as a guideline until the European Data Protection Committee has issued its own harmonized guideline in accordance with GDPR Article 70(1)(k).

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

Companies face many uncertainties. The GDPR has yet to be clarified through case law. Currently the European Commission, data protection authorities (Article 29 Data Protection Working Party) and the DSK from time to time release guidelines on how to interpret and apply the GDPR. However, these guidelines only reflect the opinion of the respective data protection authority or the DSK and thus are not binding.

It remains to be seen whether the courts, when confronted with an order, will follow the interpretation of the authority or decided differently.

GREECE

1 PRIVACY LAW

1.1 How is privacy regulated in Greece?

Privacy in Greece is, first of all, protected at a constitutional level, by article 9A of 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 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 Law No 3471/2006 (as amended), which implemented the ePrivacy Directive (or "Cookie Directive").

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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, Law No 4624/2019, 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 EU Directive 2016/680 into Greek law.

The most important provisions relating to private entities in Law No 4624/2019, which are supplemental to the provisions of the GDPR, are the following:

(a) Article 21: Consent of minors to processing of their personal data in relation to information society services;

(b) Article 22: Processing of special categories of personal data for certain purposes other than those provided in Article 9(1) of the GDPR;

(c) Article 23: Prohibition on processing of genetic data for purposes of health and life insurance;

(d) Article 25: Processing of personal data for further purposes other than those for which the data had been collected;

(e) Article 27: Processing of personal data in the context of employment;

(f) Articles 28–30: 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) Articles 31, 32: Exceptions from the obligation to inform ;data subject in specific cases (derogating from articles 13–14 of the GDPR);

(h) Articles 33, 34: Exceptions to the right of access (under article 15 of the GDPR) and to the right of erasure (under article 17 of the GDPR) in specific cases; release from the obligation to communicate a data breach to the data subject in specific cases (under article 34 of the GDPR); and

(i) Article 38: Penal sanctions for specific wilful violations of data protection law.

Law No 4624/2019 has also repealed 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, article 11 of Law No 3471/2006 provides rules for marketing communications by electronic means.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The independent supervisory authority responsible for monitoring the implementation and enforcement of privacy law in Greece is the Hellenic Data Protection Authority ("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 Article 38 of Law No 4624/2019, the penal courts are also competent to enforce the data protection rules.

2 SCOPE

2.1 Which companies are subject to privacy law in Greece?

As far as the GDPR is concerned, please see the European Union chapter.

Law No 4624/2019 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 privacy law, subject only to its territorial scope (see question 2.2).

2.2 Does privacy law in Greece apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, Greek privacy law can apply to companies outside Greece.

As far as the GDPR is concerned, please see the European Union chapter.

Greek Law No 4624/2019 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 in writing a representative pursuant to Article 27 of the GDPR (please see the European Union chapter).

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Greece?

There is no definition of "personal data" in Greek Law No 4624/2019; therefore, the GDPR definition applies (see the European Union chapter).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In relation to the "special categories of personal data" covered, primarily, in Article 9 of the GDPR, Greek Law No 4624/2019 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, Law No 4624/2019 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

The Hellenic DPA considers that the data controller is obliged to carry out a data protection impact assessment ("DPIA") in cases of systematic data processing which involves profiling of natural persons for marketing purposes, provided that the data is combined with data collected from a third party.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Greece? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Greece? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter and see question 1.2 in relation to limitations of data subjects' rights provided by Law No 4624/2019.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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 his/her valid, informed and explicit consent prior to the communication ("opt-in" system).

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 his/her prior explicit 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 the data subject to object to the collection and use of his/her contact details in the future ("soft opt-in" system). In a recent decision, the Hellenic DPA imposed a fine of 200,000 Euros to 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 recently imposed a considerable administrative fine of 200,000 Euros 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 application, 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter, question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter for the administrative sanctions.

In addition, Law No 4624/2019 provides penal sanctions for specific wilful violations of data protection law.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Greece which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The "next big thing" in privacy law is the proposed ePrivacy Regulation, which will replace the ePrivacy Directive ("Cookie Directive"). 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 cautions around processing personal information/personal data in Greece?

The Hellenic DPA has started to issue rather heavy administrative fines to companies in cases of major violations of the GDPR. See question 8.1 in relation to two fines, of 200,000 Euros each, imposed on a leading Greek telecommunications provider. Another fine, of 150,000 Euros, was imposed on the Greek company member of a multinational accounting firm for violations of the GDPR in the context of employment relations.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

The decisions and guidelines issued by the Hellenic DPA are very important for the interpretation and application of the GDPR in Greece; therefore, companies will need to seek local legal advice in case Greek privacy laws apply.

HUNGARY

1 PRIVACY LAW

1.1 How is privacy 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 (also known as the "Infotv.").

The Infotv. has two prongs. 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on advertising aspects.

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, eg:

(a) Hungarian Labour Code,

(b) Whistle-blowing Act,

(c) Act on Commercial Advertising Activities,

(d) Act on Electronic Commercial Activities,

(e) Act on Electronic Telecommunications,

(f) Act on the Processing of Health Data,

(g) Credit Institutions Act,

(h) Insurance Act, and

(i) Anti-Money Laundering Act.

For details on the legal basis of processing in a marketing context, please see question 8.1 below.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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 (Nemzeti Adatvédelmi és Információszabadság Hatóság or "NAIH"). The NAIH regularly publishes resolutions on and uploads opinions and recommendations onto its website.

2 SCOPE

2.1 Which companies are 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:

(a) to the processing of personal data if the controller has its main establishment or only place of administration within the EU in Hungary; and

(b) to the processing of personal data by a controller who has its main establishment or only place of administration within the EU 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 forms part of a filing system or is intended to form part of a filing system. In this regard, it is worth noting that the Infotv. provides that the GDPR also applies to the processing of data which does not form part of a filing system.

2.2 Does privacy law in Hungary apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes. See question 2.1 above.

Controllers or processors not established in the European Union are required to designate a representative in writing in the European Union (Article 27 of the GDPR).

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Hungary?

The GDPR contains the definition of personal data (Article 4(1)). 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The GDPR lists the special categories of personal data (Article 9) and contains rules applicable to personal data relating to criminal convictions and offences (Article 10). 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 names the possible legal bases which may be used in the context of such processing (Article 9). Special obligations in connection with processing sensitive data may include the need to prepare a data protection impact assessment ("DPIA") and to appoint of 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 organisational measures to safeguard the personal data and the rights and freedoms of the data subjects. If sensitive data are also processed, the required level of security is higher.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Please refer to the GDPR (especially Article 5). The main principles named in Article 5 are as follows:

(a) lawfulness, fairness and transparency;

(b) purpose limitation;

(c) data minimisation;

(d) accuracy;

(e) storage limitation;

(f) integrity and confidentiality; and

(g) accountability.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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; the documentation of data breaches).

Hungarian law contains special provisions with regards to, eg, data retention periods which apply to controllers.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

As regards information on data processing and the keeping of records of processing activities, the provisions of the GDPR have to be complied with.

The same applies to the designation of a DPO, since Hungarian law contains no additional requirements in addition to those included in the GDPR (Article 37(1)) concerning when the appointment of a DPO will be required.

As regards the preparation of a DPIA, the NAIH has issued a black list 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.

There is no registration obligation with the NAIH.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Hungary? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The provisions of the GDPR apply (ie, the controller and the processor are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk).

6.2 How are data breaches regulated in Hungary? What are the requirements for responding to data breaches?

The provisions of the GDPR apply (eg, the controller is required to document the 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

In addition to the rights as described in the GDPR, Hungarian law contains a special right as follows.

The Infotv. provides that the person who has been authorized, by the data subject in his/her lifetime before the controller in a public deed or in a document with full probative force, may exercise certain rights of a deceased data subject (right of access, right to rectification, right to erasure, right to restriction of processing, right to object) within 5 years from the date of the death of the data subject. Furthermore, even if the data subject did not make a legal statement in his/her life before the controller in a public deed or document with full probative force, a close relative is entitled to exercise

certain of his/her rights (including the right to rectification, right to object, right to erasure, right to restriction of processing) within 5 years from the date of their death.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Under Hungarian law:

(a) Postal marketing communications can be sent to the data subject based on his/her 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 the 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Hungarian law contains no special rules in this regard. The rules of the GDPR apply.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Hungarian law contains no special rules in this regard. The rules of the GDPR apply.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Hungarian law does not contain any special rules in this regard. The provisions of the GDPR have to be complied with. This basically means that there has to be a legitimate purpose and legal basis for processing; prior information has to be given to the data subjects in accordance with the GDPR; and the data shared has to be proportionate with the legitimate purpose wished to be achieved.

8.5 Are there specific privacy rules governing data brokers?

Hungarian law contains no special rules governing data brokers. The rules of the GDPR apply.

8.6 How is social media regulated from a privacy perspective?

Hungarian law contains no special rules in this regard. The rules of the GDPR and the practice of the EDPB and the EU Court of Justice apply.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Hungarian law contains no special rules in this regard. The rules of the GDPR apply.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The rules of the GDPR on data transfer apply.

Furthermore, by way of example, the Whistle-blowing Act contains provisions on the restriction of data. Namely, 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, for example, the Act on the Processing of Health Data also contains rules applicable to data transfers.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

In addition to the rules of the GDPR, companies need to consider whether the sector-specific laws contain additional provisions on data transfer.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The NAIH applies the sanctions as listed in the GDPR (Article 58). 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 his or her 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 EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. However, it is worth noting that Hungary took advantage of the relevant opening clause of the GDPR (Article 83(7)) and the Infotv. contains a provision pursuant to which the maximum amount of fine that may be imposed on public authorities and bodies is set at HUF 20 million (about EUR 60,000).

10.2 Do individuals have a private right of action? What are the potential remedies?

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, the data subject may request the supervisory authority to order the controller to comply with his/her 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Hungary which affect privacy?

It is worth noting that the Labour Code contains rules on the processing of biometric data and criminal data in the context of employment. In addition, the Labour Code also governs the control by the employer of the use of devices by their employees.

In Hungary, there is also a Whistle-blowing Act which contains mandatory rules governing when an entity decides to set up a whistle-blowing hotline scheme.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The draft ePrivacy Regulation is definitely a hot topic, even though one cannot be certain if there will actually be an ePrivacy Regulation and, if there will be, what it will contain. If adopted, the ePrivacy Regulation would most likely contain rules, amongst other things, on the use of cookies and the sending of direct marketing materials.

Another interesting topic is the implementation of the European Electronic Communications Code, due by 21 December 2020, which will bring over-the-top ("OTT") messaging services (like WhatsApp, Facebook Messenger) within the scope of the EU Telecommunications Regulation. This will certainly have an impact on such services and their providers.

A third topic will likely be the EU's Whistleblowing Directive. This Directive has to be implemented by the Member States by April 2021. Under the Directive (and, thus, the laws of the Member States implementing the same), for example, private entities employing at least 50 employees will be required to set up a whistleblowing system.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Hungary?

The NAIH has so far issued several fines on entities for the violation of the GDPR. The highest fine imposed was HUF 30 million (about EUR 90,000). Typically, the fines imposed range between HUF 1 million (about EUR 3,000) and HUF 10 million (about EUR 30,000) and they have typically been imposed for the violation of a data subject's rights 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 their 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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

The GDPR entered into force on May 25, 2016 and became applicable as from May 25, 2018. The GDPR was adopted mainly due to the fact that there are huge global data controllers and processors and data security and transparency is of utmost importance.

12.2 What do you envision the privacy landscape will look like in 5 years?

As a result of the 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.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The biggest challenge is probably to adapt to the regime brought about by the GDPR and to think in a data protection-cautious way.

At the same time, many of the provisions of the GDPR still need clarification through authority practice and case law.

It is an interesting question in itself whether courts will be willing to actively shape the landscape of data protection law or if they would rather uphold the decisions of the supervisory authorities and will be reluctant to go into the details of the legal issue at hand and change the decision of an authority when justified.

IRELAND

1 PRIVACY LAW

1.1 How is privacy 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 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).

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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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 to formally establish 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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The primary source for enforcement is the Data Protection Commission. That office (in various guises) has 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. It's statutory powers, functions and duties derive from the Data Protection Act 2018, the CDPR, 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 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Generally, this is covered by Article 9 of the GDPR. Further details are contained in the European Union chapter.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The European Union chapter contains the key principles and Ireland will not differ in that respect.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

This is governed by the GDPR. The European Union chapter contains the relevant information which would also be applicable in Ireland.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Key obligations arise from the GDPR and are set out in the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Ireland? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The key regulations arise from the GDPR and are set out in the European Union chapter.

6.2 How are data breaches regulated in Ireland? What are the requirements for responding to data breaches?

Again, this is set out in the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Such rights are specified in the GDPR and are set out in the European Union chapter. Additionally, individuals have the right to take separate court proceedings for an injunction and/or damages.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The principles of the GDPR apply and details are contained in the European Union chapter. Affirmative consent of the recipient is required.

Processing of personal data in the context of certain electronic communications (including, amongst other things, unsolicited electronic communications made by phone, email, and SMS) is subject to both the general laws set out in the GDPR and the specific laws set out in the ePrivacy Regulations 2011, under which the ePrivacy Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) was transposed into Irish law. The ePrivacy Regulations still apply in conjunction with the GDPR.

The key element in the ePrivacy Regulations, over and beyond the GDPR, is the confidentiality of communications. Processors cannot process the content of electronic communications beyond what is necessary for the provision of that service.

Section 30 of 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The principles of the GDPR apply and details are contained in the European Union chapter. The ePrivacy Regulations also apply (see question 8.1 above). These require prior informed consent for storage or for access to information stored on a user's terminal equipment. The user must agree to the use of such tracking technologies before the website can use them.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The GDPR will apply and provisions are as set out in the European Union chapter. There is presently an Irish Data Protection Commission investigation underway regarding online behavioral advertising, but the outcome of that investigation is, as yet, unknown.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The notice and consent requirements are established by the GDPR and are set out in the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

These are set out in the GDPR and are explained in the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

Generally, this would fall under the GDPR (see the European Union chapter). It is particularly relevant for Ireland, given that social media companies such as Facebook and Twitter have their European bases in Dublin. The Irish Data Protection Commission confirmed in late 2019 that, at that point in time, it had 11 separate investigations ongoing with Facebook or Facebook-related companies, and these included investigations regarding possible breaches of EU privacy rules.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

These are as set out in the European Union chapter on the GDPR.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Yes, these are established under the GDPR and set out in the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Again, these are set out in the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes; individuals 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Ireland which affect privacy?

No specific cultural issues relating to privacy.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Possible amendments to the ePrivacy Regulations (see the European Union chapter). Future issues that will require attention include the use of biometrics, geolocation services and geotagging and blockchain technology.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Ireland?

None, other than as set out above or highlighted in the European Union chapter.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Clearly the GDPR has changed the landscape completely. The reasons for those changes are elucidated in detail in the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

Any continuing changes are likely to be on an EU-wide basis. Brexit, and the unknowns associated with that, may change the path slightly for Ireland, given our close association with the UK as a chief economic trading partner. Additionally, changing technologies will require continuing privacy challenges.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

From an Irish perspective, companies using Ireland as their EU base face considerable uncertainty, given the lack of any significant case law yet associated with the GDPR. Companies here have to deal with the risk of complaints from many different EU Member States being taken against them in Ireland, and having to deal with such multi-jurisdictional challenges.

ITALY

1 PRIVACY LAW

1.1 How is privacy regulated in Italy?

In Italy, privacy is regulated by:

(a) Constitutional rights: Although the Italian Constitution does not contain a specific provision concerning the data protection and privacy rights, Italian commentators agree in recognizing a constitutional value to such rights, considered as inviolable human rights of new generation. Following the relevant case law on the matter, these rights may be inferred from the following Articles of the Italian Constitution:

(i) Article 2, recognising and guaranteeing inviolable human rights;

(ii) Article 3, establishing the principle of equality and granting the full development of individuals; and

(iii) Article 13, concerning the inviolable right to personal freedom.

(b) European law: From an EU regulation perspective, the main source of law is the EU General Data Protection Regulation (2016/679) ("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 provided, eg, the conditions and modalities of personal data processing carried out by public and private entities as well as data subjects' rights. It was repealed and replaced by Legislative Decree No 196 of June 30, 2003 (the "Data Protection Code").

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 Italian Data Protection Authority (the "Garante"), which also issues resolutions and guidelines aimed at interpreting the laws.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(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 as amended, with the introduction of the Articles listed below, by way of example and not limited to:

(i) Article 2-*ter*, establishing that in case 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 or regulation (in cases provided for by the law itself);

(ii) Article 2-*quater*, according to which the Garante must adopt ethical standards for the processing of genetic, biometric and health data and for data processing based on Article 6(1)(c), (e) of the GDPR;

(iii) Article 2-*septies*, according to which the Garante must adopt safety measures for the processing of genetic, biometric and health data;

(iv) Article 2-*octies*, by which the Italian Ministry of Justice must adopt a decree identifying adequate guarantees for data subjects' rights and freedoms to be adopted in processing data concerning criminal convictions and offences.

To date, some of the resolutions required by the Data Protection Code have not yet been adopted by the Garante, such as the provisions required by Articles 2-*quater* and 2-*septies*, nor has the Ministry of Justice issued a decree pursuant to Article 2-*octies* (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) EU ePrivacy Directive, which has been implemented in Title Ten of the Data Protection Code as amended;

(ii) Law No 5 of January 11, 2018 on telemarketing, specifically on the registration and functioning of the opt-out register and establishment of national prefixes for calls for statistical, promotional and market research purposes ("Telemarketing Law");

(iii) Resolution issued by the Garante No 229 of May 8, 2014 on simplified agreements to provide information and obtain consent regarding cookies ("Cookie Regulation");

(iv) Guidelines on marketing and against spam of July 4, 2013, issued by the Garante ("Guidelines on marketing and against spam").

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Italy does not have any self-regulatory body enforcing privacy law, rather, the Garante acts in this capacity. 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 to the competent criminal bodies any facts, that can be considered as crimes/felonies prosecutable ex officio, of which it becomes aware in the exercise of its duties or because of its function; and

(c) draws up an annual report on the activities it has carried out and the state of implementation of the privacy legislation.

2 SCOPE

2.1 Which companies are subject to privacy law in Italy?

See the European Union chapter.

2.2 Does privacy law in Italy apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

See the European Union chapter.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Italy?

See the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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, Article 2-*quinques* of 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, in accordance with Article 9(4) of GDPR, Article 2-*septies* of the Data Protection Code establishes that the Garante will adopt a specific resolution detailing further safety measures.

(c) with regard to the processing of data concerning criminal convictions and offences, Article 2-*octies* of 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, since the resolution concerning special categories of personal data and the decree about data concerning criminal convictions and offences have not yet been adopted, during this transitional period, the Garante has issued Resolution No 146 of June 5, 2019 in order to identify which provisions contained in five general authorizations (applicable under the former legislation for the processing of sensitive and judicial data) are still effective, as being compatibility with the GDPR and the Data Protection Code. These five general authorizations concern the following topics:

(a) processing of special categories of personal data in the employment relationship;

(b) processing of special categories of personal data carried out by associative bodies, foundations, churches and religious associations/communities;

(c) processing of special categories of personal data by private investigators;

(d) processing of genetic data; and

(e) processing of personal data carried out for scientific research purposes.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

In addition to the cases listed in Article 37 of the GDPR, Article 2-*sexiesdecies* of the Data Protection Code provides that the appointment of a data protection officer is also required in relation to the processing of personal data carried out by judicial authorities in the performance of their duties.

See also question 8 as regards privacy aspects concerning marketing.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Italy? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Italy? What are the requirements for responding to data breaches?

See the European Union chapter.

Moreover, the Garante has issued a specific form to be used in case of data breach notification, in which the information listed within Article 33(3) of the GDPR has been detailed (see Resolution of July 30, 2019 on the notification of personal data breach).

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

The Data Protection Code provides certain limitations to the exercise of individual rights. Specifically:

(a) Article 2-*undecies* states that such rights cannot be exercised where a real and concrete detriment might arise in connection with:

(i) the interests protected by the legislation against money laundering;

(ii) the interests protected by the legislation aimed at supporting victims of extortion;

(iii) the activities carried out by the parliamentary inquiry committees set up under Article 82 of the Italian Constitution;

(iv) the activities carried out by a public body other than a profit-seeking public body, where this is expressly required by a law for purposes exclusively related to currency and financial policy, the system of payments, control of brokers and credit and financial markets and protection of their stability;

(v) defensive investigations or the exercise of a right in court; or

(vi) the confidentiality of the identity of an employee who reports an offence of which he has become aware by reason of his office (ie, a whistleblower).

(b) Article 2-dodecies of the Data Protection Code provides limitations to individual rights for the protection of judicial independence and judicial proceedings. The exercise of rights and the performance of obligations may be delayed, limited or excluded under certain conditions.

(c) Article 2-*terdecies* of the Data Protection Code states that the individual rights of Sections 15–22 of the GDPR concerning deceased persons may be exercised by persons having a personal interest, or acting in the name of the data subject as his/her agent, or acting for family reasons deserving protection (although, in relation to the offering of information society services, the deceased person can expressly forbade the exercise of his/her rights by another person, by means of a written declaration presented or communicated to the data controller, provided that the deceased person's will is unequivocal, specific, free and informed). However, the exercise of such rights is not allowed when it is expressly forbidden by law.

In any case, the prohibition cannot affect the third parties' patrimonial rights arising from the data subject's death and the right to defend their rights in court.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

In addition, in the Italian framework, marketing communications are regulated by the Data Protection Code, which implements the ePrivacy Directive, and by the Guidelines on marketing and against spam.

In accordance with Article 130(1), (2) of 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 recipients' prior consent (opt-in requirement). 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, web sites or documents. The consent required for marketing communications performed by way of

automated or similar tools must be freely given, informed and specific. To this end, data controllers should inform recipients clearly and appropriately by means of a proper notice containing all the elements listed in Article 13 of 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).

Marketing messages are sometimes sent simultaneously to mailing lists; in this case, the addresses contained in the mailing list must not be visible (eg, by using the blind carbon copy).

In relation to email and mail marketing, the data subject's consent is not required in case of soft opt-in, under Article 130(4) of Data Protection Code, if the following conditions are met:

(a) the data controller uses the email provided by the data subject in the course of a previous sale of a product or service;

(b) the product or service advertised is similar to one previously sold (NB a purchase is necessary, a mere negotiation is not sufficient); and

(c) the data subject has been duly informed as to the purposes and modalities of the processing and he/she is given a simple opportunity to refuse or opt out of receiving marketing communications.

Moreover, again in accordance with the Guidelines on marketing and against spam, the email service providers must ensure mutual authentication of their servers and install filtering systems to detect spam.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

In addition, in accordance with Article 122 of the Data Protection Code and the Cookie Regulation, cookies are regulated differently according to the purposes for which they are intended to be used.

Specifically, cookies may be distinguished into three major groups: technical cookies (including browsing or session and functional cookies), analytic cookies and profiling cookies:

(a) In case of 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.

  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 the links to the webpages containing the information and consent forms relating to Third Parties Cookies when entering into the relating agreements.

(b) On the other hand, technical cookies do not require prior informed consent. The Publisher must provide notice in the modalities he/she deems most appropriate.

(c) Analytic cookies are assimilated to technical ones exclusively only when they are used:

(i) by the Publisher to collect aggregate information on the number of visitors and the pattern of visits to the website;

(ii) by third parties if 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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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, the 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", see question 8.6 below.

Finally, concerning profiling cookies, please refer to question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

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) The user receives a marketing message from a company that has obtained his/her personal data from his/her public profile on a social network: In this case, the data processing is unlawful unless the sender can show proof of the recipient's prior, specific and free consent under the terms of Article 130(1), (2) of 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 recipient, by his/her behavior, also intended to express his/her 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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

In addition, an 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 (Article 167 of the Data Protection Code).

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

In addition, Article 2-*decies* 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 (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 up to Euro 1,549 or up to one year's imprisonment (or, in severe cases, both)).

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Italy which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Considering the Garante's 2018 annual report (the annual report for 2019 is not available yet), it is possible to highlight the following as hot topics:

(a) With regard to the protection of personal data in the public and private employment relationship, the Garante ruled several times on data processing carried out by means of devices which allow the tracking of the geographical location of vehicles and smartphone/tablet and therefore, indirectly, the location of the employees to whom such devices are entrusted for work.

With reference to the geolocation of company vehicles, the Garante prohibited further processing of data relating to employees through the use of a vehicle location system. Indeed, it is considered in breach of the principles of necessity and proportionality with respect to the pursued purposes.

(b) As regards marketing, profiling and processing of personal data, the Garante received thousands of reports. In addition, the Garante has recently updated the FAQs relating to unsolicited advertising calls, which provide also clarification on how to object.

In this field, please note that, following the Telemarketing Law, work is continuing for the adoption of the Presidential Decree aimed at amending the regulations in force on the registration and operation of the "do not call" register and repealing any regulations that are not in compliance with the current regulatory framework.

(c) The Garante issued an opinion on the draft Guidelines for access for scientific purposes to elementary data of Sistan (ie, the national statistical system).

Finally, please consider that a fundamental hot topic is the draft EU ePrivacy Regulation. See, further, 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 cautions around processing personal information/personal data in Italy?

To date, the Garante has issued few fines in relation to GDPR enforcement. Firstly, a fine of Euro 50,000 in respect of a failure to adopt adequate safety measures regarding the processing of users' data of a web platform, in breach of Articles 32 and 83(4) of the GDPR.

Moreover, in January 2020, the Garante issued the highest fines ever (Euro 11.5 million and Euro 27 million) against two big players in the utilities field (energy and telco) for different unlawful behaviors, several of them connected with marketing (including telemarketing) and profiling.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

LUXEMBOURG

1 PRIVACY LAW

1.1 How is privacy 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 new 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The main source for data protection in Luxembourg is the GDPR.

In addition, the Law of August 1, 2018 provides for special rules for certain types of processing; e-privacy aspects are specifically regulated; and the advertising sector has adopted a self-regulatory framework. For other sector-specific laws, see question 1.1.

(a) **The Law of August 1, 2018**

The Law of August 1, 2018 contains specific rules for the following types of processing:

(i) *Personal data processing for the purposes of surveillance in the employment context:* The processing of employees' personal data for surveillance purposes can be carried out only in the cases mentioned in Article 6(1) of the GDPR and in compliance with the Labor Code.

For such processing of personal data, including video surveillance, the employer must, prior to data processing, inform the employee(s) concerned and the staff representatives (or, in certain cases, the Labor and Mines Inspectorate). The information given must contain a detailed description of the purpose(s) of the proposed processing, the modalities of implementation of the surveillance system and, if appropriate, the retention period of personal data or the criteria to determine that period, as well as a formal commitment of the employer not to use the data collected for a purpose other than that explicitly provided for in the prior notification.

In addition, data processing carried out for compliance with health and safety provisions, for monitoring the production process or employees' performance (where such processing is the only means to determine the employees' salary), or for implementing and monitoring a flexible-time arrangement, is subject to a joint decision-making process between the employer and the staff delegation, except where such data processing is required for compliance with a legal obligation.

Moreover, in all cases of processing employees' personal data for surveillance purposes, the staff representatives, or, in the absence of such representatives, the employees concerned, may, within 15 days after being given the advance information, submit a request to the CNPD for a prior opinion on the compliance of the envisaged processing. The CNPD then has to give an opinion within a month of the referral, during which time, matters are suspended.

(ii) *Processing and freedom of expression and information:* Controllers who process personal data for the sole purpose of journalism or academic, artistic or literary expression are exempt from the following rules:

- 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*: The legislator has specified appropriate safeguards in respect of processing of personal data for scientific or historical research purposes or statistical purposes. These measures include, notably, the appointment of a data protection officer, the performance of an impact assessment, use of anonymization and pseudonymization techniques, promoting the awareness of the staff involved about the processing of personal data and professional secrecy. The data controller must be able to justify any derogation from these safeguards.

Provided that these measures are implemented, 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.

(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.

The aforementioned rules on the specific processing purposes apply to all data controllers and data processors established in Luxembourg.

Under the Law of August 1, 2018, the certification bodies must be accredited by the CNPD.

(b) E-privacy

E-privacy aspects are regulated in Luxembourg by two main instruments:

(i) 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");

(ii) The law of August 14, 2000 on electronic commerce ("Electronic Commerce Law").

See, further, question 8.1.

(c) Self-regulatory frameworks

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 8.3).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

(a) Regulators

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 Article 58 of the GDPR, notably:

(i) to carry out investigations,

(ii) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks,

(iii) to issue warnings,

(iv) to impose a temporary or definitive limitation, including a ban, on processing, and

(v) to advise the controller in accordance with the prior consultation procedure.

In addition, the CNPD may impose administrative fines as set out in Article 83 of GDPR 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 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 the above.

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.

(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 ("CLP"). Any advertiser may become a member of the CLP provided a membership fee is paid.

2 SCOPE

2.1 Which companies are subject to privacy law in Luxembourg?

See the European Union chapter.

2.2 Does privacy law in Luxembourg apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

As to the provisions of the GDPR, see the European Union chapter.

The rules on specific processing purposes (eg, processing of employee data for surveillance purposes) under the Law of August 1, 2018 apply only to data controllers and data processors established in Luxembourg.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Luxembourg?

See the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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(a).

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

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 Article 35 of 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Luxembourg? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Luxembourg? What are the requirements for responding to data breaches?

See the European Union chapter.

The CNPD published on its website a data breach notification form to help companies to notify data breaches in due time.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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. The following do not in themselves constitute commercial communications:

- information allowing direct access to the activity of the company, organization or person, in particular a domain name or an electronic-mail address;
- 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.

Commercial communications must comply with the following requirements:

(a) commercial communications must be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communications is 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 from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these 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 electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such. This exception must be interpreted restrictively.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

Regarding sanctions for breach of the provisions of the Law of August 1, 2018:

(a) 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 five per cent of the average daily turnover generated by the data controller or data processor during the last financial year per day of delay;

(b) 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 between 251 and 125 000 euros; and

(c) 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 euros and/or imprisonment of up to one year.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Luxembourg which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

There are two hot topics in the privacy landscape at the moment:

(a) Brexit: Considering the uncertainties surrounding a data flows deal with the United Kingdom, the CNPD has published guidelines on the consequences of Brexit for international data transfers. These guidelines aim to help companies, public bodies and Luxembourg associations that are transferring personal data to the UK.

Companies concerned should determine which of the GDPR appropriate guarantees is best suited for their organization, and should ensure that such guarantees are in place by January 31, 2020.

According to the CNPD, the conclusion of standard data protection clauses between the Luxembourg entity in question and the UK data importer may be the best option for businesses.

(b) Certification schemes: In July 2019, the CNPD published an updated draft version of the accreditation requirements for certification bodies that wish to certify data processing operations according to the criteria of GDPR-CARPA.

The final versions of the accreditation requirements for certification bodies, the certification mechanism, and the certification criteria of GDPR-CARPA will be published after obtaining the opinion of the European Data Protection Board.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Luxembourg?

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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

The entry into application of the GDPR was accompanied by an increased awareness among professionals and individuals about privacy challenges, and has led to a significant increase in inquiries with the CNPD.

According to the CNPD's 2018 annual report, the number of written requests and complaints doubled compared to previous years. Most complaints concerned the rights of data subjects (right to access and right to be forgotten), the retention periods, and the compliance of general terms and conditions of e-commerce websites with the new data protection rules.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

In 2018, the CNPD started to implement proactive investigations. These investigations are carried out in the form of thematic audits on the new obligations under the GDPR. For instance, in 2018, several audit procedures were commenced to check the compliance of data controllers with the rules concerning the appointment of data protection officers.

THE NETHERLANDS

1 PRIVACY LAW

1.1 How is privacy 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 came into force in May 2018. The GDPR covers all aspects of privacy law concerning the processing of personal data.

On 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 in Article 10(1) as the right to respect for his/her privacy. 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.

The second and third paragraphs of Article 10 include two mandates given to the legislator: the legislator must establish laws that provides rules for the protection of privacy regarding the recording and provision of personal data; and the law must regulate the right of access and the right to correct inaccurate personal data. The GDPR accommodates most of the legislation required by Article 10(2), (3) of the Dutch Constitution. Other aspects are covered by the Dutch GDPR Implementation Act ("Implementation Act") and, for national security and processing of personal data for the detection and criminal prosecution, in the Police Data Law and Judicial and Criminal Records Law ("WJSG").

Together with the GDPR, the Netherlands has adopted the Dutch Implementation Act. The GDPR and Implementation Act replaced the Personal Data Protection Act ("Wbp") that was an implementation of the EC Data Protection Directive and largely regulated privacy on a national level.

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.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The GDPR forms the primary source for data protection in the European Union and therefore in the Netherlands. The GDPR, as any EU Regulation, is directly applicable in all EU Member States and does not have to be implemented. The GDPR covers most aspects of data protection. However, the GDPR contains a couple of opening clauses, permitting EU Member States to introduce (more restrictive) national rules on certain privacy aspects.

The Implementation Act broadly covers two topics: firstly, it establishes the position and powers of the Dutch data protection authority ("AP") as the supervisory authority. And secondly, it gives substance to the opening clauses regarding the special categories of personal data.

Certain aspects of marketing activities, including direct marketing by e-mail or telephone are regulated in the Telecommunications Act (see question 8.1).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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.

The Netherlands does not have any self-regulatory bodies that enforce privacy law.

2 SCOPE

2.1 Which companies are subject to privacy law in the Netherlands?

See European Union chapter.

In addition to the scope of the GDPR, the Implementation Act applies to companies, who control or process personal data, which 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 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 INFORMATION

3.1 How is personal information/personal data defined in the Netherlands?

"Personal data" is defined by Article 4(1) of the GDPR (see European Union chapter).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The categories of personal data that are considered sensitive can be found in Article 9(1) of 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.

In addition to the exemptions to process sensitive personal data as defined in the GDPR, Articles 22–30 of the Implementation Act provide exceptions that legitimize the processing thereof. There are exceptions concerning:

(a) processing necessary for the fulfilment of legal obligations;

(b) processing personal data revealing racial or ethnic origin;

(c) processing personal data revealing religious beliefs;

(d) processing of genetic data;

(e) processing of biometric data;

(f) processing of data concerning health; and

(g) processing of data relating to criminal law matters.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in the Netherlands? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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.

6.2 How are data breaches regulated in the Netherlands? What are the requirements for responding to data breaches?

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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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 in the sense of Article 6 of the GDPR. 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.

Three types of direct marketing can be identified, each with their own set of rules under the Telecommunications Act:

(a) *Digital direct marketing*: The general rule is that digital direct marketing can only be sent (by email, text or WhatsApp) if prior consent has been obtained from the data subject. There is one exemption to this rule, namely that permission is not required for offers aimed at existing customers, provided that the offer concerns the company's own, similar products.

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.

(b) *Telemarketing*: The general rule for telemarketing is that, if the personal data is required legitimately, permission is not required to telephone a data subject. However, the Telecommunications Act contains two exemptions to this rule:

(i) if the data subject has invoked the right to object to the use of their personal data for telemarketing purposes, the company is no longer allowed to call the data subject in question; and

(ii) if the telephone number of the data subject is listed in the Do Not Call Registry, although this exemption does not apply to existing customers, whom the company is allowed to call with an offer for their own, similar products and services. However, under all circumstances and during every conversation, the data subjects should be made aware of their right to object and the possibility to register in the Do-Not-Call-Register.

(c) *Advertising by post*: The last category of direct marketing as defined in the Telecommunications Act is advertising by post. Different rules apply to existing customers and future customers. However, if the data subject has invoked his/her 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 send 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 that the company should have a legitimate interest (Invoking this GDPR basis is not excluded according to recital 47 of the GDPR).

(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.

Besides the provisions of the Telecommunications Act, two self-regulating codes are applicable in the Netherlands to marketing communications: the Email Code 2012 and the Telemarketing Code 2012 ("CTM"). The Email Code applies to unsolicited advertisements via email, and the CTM applies to telephone conversations between telemarketer and consumers, where consumers are telephoned using a Dutch telephone number.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

In addition to the GDPR rules, the Netherlands has a stricter regime that applies to the use of tracking cookies. This stricter regime follows from the Telecommunications Act.

The use of tracking technology is regulated in the Telecommunications Act, which implemented the ePrivacy Directive.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter question 8.2.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

In addition to the penalties and sanctions set out in the GDPR, the following additional penalties and sanctions are available in the Netherlands for violations of the GDPR:

(a) the maximum administrative fine can be imposed for violation of Article 10 of the GDPR (personal data relating to criminal convictions and offences); and

(b) fines may also be imposed on public authorities.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of the Netherlands which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

See the European Union chapter.

The hottest topic is the draft ePrivacy Regulation, because when it enters into force it will replace the Telecommunications Act.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in the Netherlands?

After a period of restraint, the AP has started to take the following enforcement actions:

(a) as of January 1, 2020, it has imposed a ban on the processing of national identification numbers by the Dutch Tax Authority;

(b) it imposed an incremental penalty payment on the Employment Insurance Agency (a government agency) for not implementing the appropriate security measures for the employer login portal; and

(c) it imposed a fine on the Haga Hospital for failing to have the internal security of its patient files up to standard.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See European Union chapter.

POLAND

1 PRIVACY LAW

1.1 How is privacy 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 Data Protection Directive 95/46/EC 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 regulator etc);

(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 more broadly discussed below.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on advertising aspects.

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) Article 2: 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) Articles 3–5a: conducting public services by data controllers — if related to the performance of public duties — is exempted from complying with certain obligations (eg, to provide privacy notices and respond to subject access requests);

(c) Article 6: the processing of data by entities in the public finance sector are fully exempt if such processing is necessary to perform tasks in the interests of national security;

(d) Article 6a: performance of constitutional and statutory competences of the President of the Republic of Poland, to the extent 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. In this regard the Amending Act has introduced many changes, including changes to the laws regulating marketing activities. It specifically addresses the provisions on the consent which must be collected from subscribers or end users, and which has to 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 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 the personal data protection; eg, one describes the regulator's approach to data breaches. The guidelines are available, in Polish, on the official website of the PDPO.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The PDPA established a new supervisory authority — the President of 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.

In addition to the powers set out in Article 58 of the GDPR, the PDPO has some additional powers; eg, 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.

Pursuant to the PDPA, the President of the PDPO is entitled to carry out inspections regarding compliance with personal data protection regulations. Such inspections are carried out by a person authorized by the PDPO President, being an employee of the PDPO or a member or an employee of a supervisory authority of an EU Member state. Such inspection must meet some legal requirements (eg, with regard to time frame).

Please note, that there is no self-regulatory body in Poland enforcing the privacy law.

2 SCOPE

2.1 Which companies are subject to privacy law in Poland?

See the European Union chapter.

2.2 Does privacy law in Poland apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 Article 3 of the GDPR. There are no other specific national provisions governing this issue.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Poland?

The PDPA does not provide any local derogations from the definitions set out in GDPR. Therefore, "personal data" should be understood in accordance with the definition contained in the Article 4(1) of GDPR (see the European Union chapter).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In addition, Polish regulations on personal data protection contain specific rules on processing of sensitive personal data with respect to the following entities:

(a) 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 the 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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

Pursuant to the obligation deriving from the Article 37(7) of the GDPR, the PDPA provides for a notification obligation regarding the designation of a data protection officer ("DPO"). The designation of a DPO must be notified to the President of the PDPO within 14 days from the date of the designation. The notification should be drawn up in electronic format and requires a qualified electronic signature or a signature confirmed by a Polish trusted profile at the ePUAP (Polish Electronic Platform for Public Administration Services), which is a free-of-charge method of authentication of a citizen's identity in e-governmental systems.

Furthermore, the controller or processor must make, immediately after the designation, the data concerning the DPO available on its website or in a generally accessible manner at a place of pursuit of activity.

In the event of the designated DPO's absence, a person may be appointed to act as a DPO (a deputy). The appointment of a deputy DPO should be notified to the President of the Office in the same way as that for a DPO.

In addition, the PDPA specifies which "public authorities" must appoint a DPO; namely: units of the public finances sector, research institutes and the National Bank of Poland.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Poland? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Poland? What are the requirements for responding to data breaches?

Under the PDPA, the PDPO has a competence to introduce an online system enabling controllers to report data breaches. However, at present, no such system is available.

Instead, data breaches can be notified to the PDPO electronically by completing a form available on the PDPO's website. The notification must be submitted in Polish. In case of a cross-border data breach,

the controller must analyze whether the lead supervisory authority regarding processing activities covered by the breach is the PDPO or another European supervisory authority.

Please note, that EU Regulation 611/2013 on the notification of personal data breaches is directly applicable in Poland. Therefore, some additional data breach notification obligations apply to providers of publicly available telecommunications services (eg, shorter period of time for responding to a personal data breach).

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter.

With respect to marketing communications, not only data protection law, but also the Act of July 16, 2004 on Telecommunications ("TL") and the Act of July 18, 2002 on the Provision of Electronic Services ("APES") must be taken into account.

Due to the entry into force of the Amendment Act, some provisions of the TL and APES have been changed. The main amendments refer to the consent of subscribers or end users, which has to comply with the provisions on personal data protection. For example, consent is required in order to:

(a) use telecommunications terminal equipment and automated calling systems for the purposes of direct marketing; or

(b) send commercial information by electronic means of communication, including, but not limited to, electronic mail.

Therefore, sending commercial information (eg, by email or SMS) to a natural person is permitted solely upon the recipient's prior consent, which cannot be presumed and can be revoked at any time. The same applies to direct marketing using end telecommunications devices or automated calling systems.

According to a recent decision of the President of the Office of Competition and Consumer Protection (which is the Polish authority responsible for consumer protection policy), such consent must be obtained from the consumer separately from consent regarding general processing of personal data (Decision No DOZIK-8.610.20.2017.KA/MO).

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

Concerning cookies, it is necessary to provide subscribers or end users with information related to:

(a) the purpose for which the information is stored and accessed; and

(b) the possibility of defining the conditions under which this information is stored and accessed, by adjusting the settings of the software or the configuration of the service.

Cookies can be used, provided that the subscriber or user concerned gives his/her consent, which may be expressed by means of service configuration or the settings of their software or browser. As already mentioned above, the consent has to meet data protection requirements.

What is more, the stored information or the access to such information must not cause changes in the configuration of the subscriber's or end user's telecommunications terminal equipment, or of any software installed on that equipment.

The above rules are not applicable where the storage of and access to the information is necessary to perform a transmission through a public telecommunications network or provide a telecommunications service or an electronically supplied service requested by a subscriber or end user.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter and question 8.2 above.

With the customer's permission, a service provider may process other data concerning such customer that are not necessary to provide a given service by electronic means, but is 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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union Chapter.

With regard to the transfer of personal data outside the country or between group companies, the PDPA does not impose any additional requirements, such as notification or reporting obligations to the President of the PDPO.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union Chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union Chapter.

The PDPA introduces 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 100,000 PLN (approximately EUR 23,400).

According to the data available on the official website of the PDPO, to date, the PDPO has imposed five administrative financial penalties for noncompliance with personal data protection rules or failure to take sufficient measures to ensure information security (four of the five have been enforced against entities from the private sector).

In addition to administrative liability, the PDPA sets forth criminal provisions and sanctions. Criminal sanctions may be imposed on a given entity for:

(a) processing personal data if such processing is not allowed or the processing is carried out without authorization; or

(b) 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).

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union Chapter.

Individuals may challenge the violation of their personal data through civil proceedings.

Pursuant to Article 92 of the PDPA, the provisions of the Polish Civil Code apply to claims arising from a breach of the personal data protection provisions set forth in the GDPR.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Poland which affect privacy?

According to the Act of October 7, 1999 on the Polish Language, consumers have to be informed in Polish. Therefore, any privacy notices, which are addressed to consumers, have to be in Polish.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

According to the PDPO's sectoral control plan for 2020, the President of the PDPO has decided to check the level of compliance with the data protection law in banks (regarding copying ID documents) and in those entities which use remote water reading systems.

What is more, pursuant to information obtained from the PDPO, it is very likely that an agreement on unwanted telemarketing calls will be concluded between the President of the PDPO, the President of the Office for Competition and Consumer Protection and the President of the Office of Electronic Communications. Please note, that no official information on this subject has yet been released.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Poland?

In Poland, there is, as yet, no current common enforcement practice in relation to the GDPR. However, the activity of the President of the PDPO has recently increased and it may be expected that it will keep on rising in 2020.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Since the GDPR came into force, there has been a rapid increase in complaints lodged with the PDPO. Based on data revealed by the PDPO, about 2,700 complaints were lodged in 2017, while in 2018 this number reached almost 4,500. In 2019 it has increased to the level of approx 7,000. Bearing that in mind, the PDPO has introduced changes in its structure in order to improve its operations in this area. New departments have been set up within the PDPO, such as a Complaints Department to handle exclusively citizens' complaints, and the Inspections and Breaches Department to handle personal data protection breaches reported by controllers and the conduct of inspections at controllers. Also, taking into account the rising awareness in Poland of the protection of personal data, a new Communication Department has been established, whose tasks include informing citizens effectively about their rights (eg, by use of hotlines).

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Many companies in Poland are still waiting for the development of guidelines and standards for the establishment of appropriate means of protecting personal data within their business activities. The

PDPO has so far issued only a few guidelines which cover some issues connected with the application of the data protection regulations in Poland. They are all available on its official website.

PORTUGAL

1 PRIVACY LAW

1.1 How is privacy regulated in Portugal?

Privacy is regulated by statutory law, such as constitutional rights, national law and European law. All this legislation is interpreted and enforced by the Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados Pessoais, "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 the decisions and/or the administrative offence proceedings related to data protection matters.

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 (see question 1.2).

In addition to the guidelines issued by the Portuguese DPA, also the guidelines issued by the European Data Protection Board may also be used by the legal and judicial operators when dealing with privacy matters.

Finally, there are specific privacy stipulations in other sectorial laws.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The main legal source for data privacy protection is the GDPR.

At a national level, the GDPR Implementation Law establishes specific requirements applicable to:

(a) employment relationships (article 28);

(b) a child's consent (article 16) (see further question 3.2(a));

(c) personal data of deceased persons (article 17) (see further question 3.2(b));

(d) portability and interoperability/interconnection of data (article 18);

(e) video surveillance (article 19);

(f) rules applicable to data protection officers (articles 9–13); and

(g) health and genetic data (article 29) (see further question 3.2(c)),

among others.

However, the Portuguese DPA issued Deliberation No 2019/494 on 3 September, according to which it states that it will not apply the following 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:

(a) article 28(3)(a) (employee consent is not a lawful ground for data processing where processing results in a legal or economic advantage for the worker),

(b) article 2(1), (2) (territorial scope of the legislation) (see further question 2.2),

(c) article 20(1) (duty of secrecy overrides rights to information and access to data),

(d) article 23 (processing/transmission of personal data by public entities for purposes other than those for which data was collected) (see further question 4.1),

(e) articles 37(1)(a), (h), (k), (2), 38(1)(b), (2) (certain offenses) (see further question 10.1),

(f) article 39(1), (3) (criteria for setting amount of fine),

(g) article 61(2) (expiry of consent) and

(h) article 62(2) (date of ineffectiveness of rules on authorizations and notifications to DPA).

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 (see further question 8). The legal framework applicable to unfair commercial practices also regulates certain aspects of marketing activities.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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 article 57 of 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 remedy and sanction non-compliance;

(c) makes available a list of data processing activities subject to a data protection impact assessment, under paragraph 4 of article 35 of the GDPR;

(d) prepares and submits to the European Committee for Data Protection, the criteria projects for the accreditation bodies for monitoring of codes of conduct and certification bodies, under articles 41 and 43 of the GDPR; and

(e) cooperates with the Portuguese Institute for Accreditation, under article 14 of the GDPR Implementation Law.

The Portuguese DPA exercises the powers established in article 58 of the GDPR.

2 SCOPE

2.1 Which companies are subject to privacy law in Portugal?

See the European Union chapter.

Building on article 2 of the GDPR, article 2(3) of the Portuguese GDPR Implementation Law specifically establishes that it 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

See the European Union chapter.

By article 2(1) of the GDPR Implementation Law, the GDPR Implementation Law applies to the processing of personal data carried out in Portugal and, in some circumstances, to the processing of personal data carried out outside the Portuguese territory (article 2(2)).

However, the DPA has decided that it will not apply these provisions in future cases, as it considers that such rules violate GDPR dispositions, in particular GDPR articles 3 and 56.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Portugal?

See the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

In addition to the obligations contained in the GDPR, the GDPR Implementation Law specifically establishes specific requirements related to processing of special categories of personal data. We highlight the following ones:

(a) Child's consent (article 16): By article 8 of the GDPR, 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 him/her, 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 (article 17): personal data of deceased persons are protected under the GDPR when such data falls within the special categories of personal data under article 9(1) of the GDPR or when the data relates to privacy, image or to communications, except as provided in GDPR article 9(2). The deceased person's rights provided for in the GDPR, namely the right of access, rectification and erasure, may be exercised by the person so designated by the deceased person or, failing that, by his/her heirs. The data subject may instead determine that no-one may exercise such rights after his/her death.

(c) Health and genetic data (article 29): 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. This article also imposes a duty of confidentiality on persons who have access to health data.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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 by the data collection. The basis for processing 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 by the 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 article 5(1)(b) of the GDPR (see question 1.2).

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

The Portuguese GDPR Implementation Law stipulates that it is mandatory for private entities to appoint a data protection officer where their main private activity involves data processing which requires the regular and systematic monitoring of data subjects on a large scale, or data processing on a large scale of special categories of data, or of personal data related to criminal convictions and administrative offences.

Public bodies which are obliged to appoint a data protection officer are (i) the State; (ii) the Autonomous Regions (Azores and Madeira); (iii) local authorities and other bodies provided for by law; (iv) independent administrative entities; (v) the Bank of Portugal; (vi) public institutes; (vii) public higher education institutions; (viii) State-owned and regional and local business enterprises; and (ix) public associations.

The performance of the data protection officer's duties does not require professional certification and, regardless of the nature of the legal relationship with the data controller, the data protection officer maintains technical autonomy.

In addition to those given in articles 37–39 of the GDPR, the data protection officer shall have the following tasks:

(a) ensure that periodic and unscheduled audits are carried out;

(b) make users aware of the importance of early detection of security incidents and of the need to immediately inform the security officer; and

(c) ensure relations with the subjects on matters covered by the GDPR and by the national legislation on data protection matters.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Portugal? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Portugal? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter.

In addition, the legal framework applicable to direct marketing in Portugal is mainly based on Law No 41/2004, of August 18, last amended by Law No 46/2012 of August 29 ("E-Privacy Law") that implemented the EC ePrivacy Directive and is applicable to direct marketing through automated means (sms, mms, ems, automated calls and fax) and electronic mail.

Please note that the E-Privacy Law does not distinguish between private and professional customers, but between natural and legal persons.

By this Law, the sending of unsolicited direct marketing communications to a natural person, through automated means which do not depend on human intervention, is subject to the prior and express consent of the user (opt-in). Consent must meet the requirements laid down in article 7 of the GDPR.

However, it is possible to send marketing communications to legal entities without prior consent (opt-out), provided that:

(a) the legal entity is not included in the official list of legal entities that oppose the receipt of such communications; and

(b) the legal entity is given the opportunity to oppose the receipt of such communications.

With respect to existing customers, in cases where the data controller has already obtained personal data of the customer, the law allows for the sending of marketing communications aiming to promote the data controller's own or similar products, provided that the customer is given the chance to oppose the receipt of marketing communications at the time of the data collection or, in cases where the customer has not initially refused the processing of their data for marketing communications, in each communication (soft opt-in).

Note that article 21(2) of the GDPR also applies (see the European Union chapter).

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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 his/her 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 him/her. 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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

The Portuguese GDPR Implementation Law establishes that the protection of personal data must not affect the freedom of speech, 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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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 under article 49(4) of the GDPR.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

The Portuguese GDPR Implementation Law provides for additional administrative offences to those provided for in the GDPR. However, the Portuguese DPA has decided (see question 1.2) that it will not apply some of these in future cases, due to the fact that it has considered that they violate article 83(4), (5) of the GDPR.

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).

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.

The GDPR Implementation Law specifies (in articles 46–53) several crimes with regard to personal data, such as:

(a) the use of data incompatible with the purpose of the collection;

(b) improper access;

(c) data diversion;

(d) data corruption or destruction;

(e) insertion of false data;

(f) breach of the duty of confidentiality; and

(g) 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 provided for in Law No 67/98 of 26 October (the former Portuguese Data Protection Law), except for the crime of violation of the duty of professional confidentiality, whose maximum limit is reduced by half.

Attempting to commit such crimes is also always punishable.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Portugal which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

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 cautions around processing personal information/personal data in Portugal?

The Portuguese DPA has started to bring administrative offense proceedings:

(a) In particular, it has imposed a fine of 400,000 Euros 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) It has imposed a fine of 107,000 Euros on a consumer protection association for sending unsolicited emails for direct marketing or advertising purposes without obtaining prior consent (Article 6 of the GDPR and article 13-A of the E-Privacy Law).

(c) A fine of 20,000 Euros was imposed on a car brand for denial of the right of access to recorded phone calls by the data subject.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

With the entry into force of the Portuguese GDPR Implementation Law, it is expected that the Portuguese DPA will initiate random audits to check compliance with data protection law on a more frequent basis, as well as carry out audits initiated by individual complaints.

Additionally, we also envisage an increase in claims from a data protection law and consumer protection law perspective.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

Companies and judicial and legal operators may face uncertainties caused by the decision of the DPA, which has decided that it will not apply several provisions of the Portuguese GDPR Implementation Law (see question 1.2). This decision has not yet been analyzed and/or clarified by the Portuguese courts.

ROMANIA

1 PRIVACY LAW

1.1 How is privacy regulated in Romania?

In Romania, privacy is regulated by statutory law, the right to privacy being stated as a constitutional right. Moreover, the right to privacy is reinforced in the Romanian Civil Code as well as several qualified laws, applying the related EU provisions.

Ensuring the right to privacy to its citizens has always been a major concern for the Romanian statutory bodies, which have shown, over time, great attention to this subject by strictly regulating methods of enforcing it.

The Romanian Constitution establishes in Article 26 that "The public authorities are deemed to respect and protect the intimate, family and private life."

The Romanian Supreme Court has also shown 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."

The previous EC Data Protection Directive was applied in Romania by Privacy Law No 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, (now repealed), which was then the main legal instrument for the protection of the data subjects' rights.

Currently, the open clauses of the GDPR are implemented in Romania through Law No 190/2018 on GDPR implementing measures ("Privacy Law"), 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"), that aligns the Romanian supervisory authority's powers with the GDPR, as well as several guidelines issued by the Romanian supervisory authority, the National Supervisory Authority for Personal Data Processing ("ANSPDCP").

Law 129/2018 mostly contains administrative stipulations and relevant aspects on the enforcement of the provisions of the GDPR and of the national legislation, whilst the Privacy Law implements, as its name provides, the open clauses of 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") regulates the communications sent through the public electronic communication networks and through the electronic communication services provides certain requirements that need to be complied with when sending electronic communications to data subjects.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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.

The main provisions established by the Privacy Law, when implementing the open clauses of GDPR concern the following aspects:

(a) 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;

(b) how public authorities are treated in comparison to private operators with respect to enforcing data protection provisions;

(c) data processing at work; and

(d) 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.

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, emphasizing the provisions of Article 6 of the GDPR, stating that a natural person should receive electronic communications (or any other type of communications) only upon granting consent.

Additional provisions on commercial communications are regulated by Law No 365/2002 regarding electronic commerce ("Law 365/2002"), that alongside the GDPR, establish that sending electronic communications is forbidden if a natural person did not give his/her prior consent.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

All aspects concerning privacy are enforced by ANSPDCP, the Romanian supervisory authority. In this respect, ANSPDCP can perform investigations at a controllers' headquarters in order to establish whether privacy laws are adequately implemented; and can issue sanctions, including fines, when infringements of data protection provisions are observed.

2 SCOPE

2.1 Which companies are subject to privacy law in Romania?

Privacy law applies to both public and private controllers and processors. However, public authorities and bodies benefit from a preferential treatment when it comes to sanctions. Only public entities have a 90-day period, from the report identifying and sanctioning the infringement, for the remediation and the fulfillment of the legal obligations, while private entities do not benefit from such a grace period.

2.2 Does privacy law in Romania apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 INFORMATION

3.1 How is personal information/personal data defined in Romania?

The Romanian legal provisions have not defined "personal data", given that it is already defined in Article 4(1) of the GDPR.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 implement the following safeguards:

(a) implement the 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;

(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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

Moreover, if special categories of personal data are processed on a large scale for advertising purposes, a data protection impact assessment is required.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Romania? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The GDPR imposes the general framework regarding the standard required in ensuring the security of personal data.

Companies, as well as public authorities and bodies, also have, as an instrument in implementing the adequate security standard, the consultation procedure with ANSPDCP. Therefore, these entities can file a formal letter to the national supervisory authority with respect to a certain type of processing, requiring advise in order to ascertain the proper method of establishing the security of personal data.

6.2 How are data breaches regulated in Romania? What are the requirements for responding to data breaches?

Complementary with the GDPR, ANSPDCP has issued a form for notifying data breaches, helping controllers to comply with all the legal requirements in order to ensure that the breach is handled correspondingly.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter, and see question 1.1 above.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter.

Additionally, Law 506/2004 and Law 365/2002 establish that explicit consent is required for a natural person to receive electronic communications.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Processing personal data for targeting purposes and in order to analyze the behavior of data subjects in relation to certain advertising campaigns has always been a sensitive subject from the legal perspective.

Data subjects must be properly informed when they are subject to profiling and, if consent is required, only explicit consent is permitted.

Moreover, in order to ensure an adequate balance between the rights of data subjects and the right of the controller, performing a data protection impact assessment is recommended, if not, in some cases (eg, processing on a large scale, processing sensitive data) mandatory.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

In addition, the Privacy Law, as well as certain procedures issued by ANSPDCP, establish that any case handler can issue a fine up to EUR 300,000 when performing an investigation at a controller's headquarter if an infringement occurs, without any prior approval from the president of ANSPDCP.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Romania which affect privacy?

Not applicable.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

As for every Member State of the European Union, the draft of ePrivacy Regulation is a subject that constantly needs to be followed in Romania. Please 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 cautions around processing personal information/personal data in Romania?

ANSPDCP has issued several fines on Romanian companies, as well as on a flat owners' association. Most of the fines concerned the inadequate, or failure to implement the adequate, technical and organizational measures.

So far, no specific guideline on imposing fines has been issued, yet the sanctions imposed on the infringing entities were way below the threshold of either EUR 20 million or EUR 40 million.

Generally, the sanctions imposed on the entities have not exceeded the amount of EUR 130,000.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Although the GDPR and the national provisions regulate many aspects of data privacy, the level of diligence that companies must have in order to comply with the data privacy requirements is not yet clearly regulated.

Until a strong base of case law becomes available, all that entities can do is to perpetually comply with an on-going process of alignment with the data privacy provisions and established practice.

SLOVAKIA

1 PRIVACY LAW

1.1 How is privacy regulated in Slovakia?

Privacy is primarily regulated by European law, namely European 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 Col on Personal Data Protection ("DPA").

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Key laws regulating privacy in Slovakia are the GDPR and the DPA.

The GDPR is directly applicable in Slovakia and therefore most processing activities are governed by the rules and principles contained in the GDPR.

The DPA 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 DPA is therefore the alignment of the Slovak national legislation on data protection with the GDPR. At the same time, the DPA 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 DPA also represents a transposition into Slovak law of Directive 2016/680/EU on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating, detecting or prosecuting for the purpose of enforcing criminal sanctions and on the free movement of such data. Lastly, the DPA regulates the status, scope and organizational structure of the Slovak Data Protection Office ("DPO").

While the processing of personal data is governed by the GDPR and the DPA, certain privacy aspects of online marketing activities, such as direct marketing by email or telephone, are also regulated by other laws, including in particular the Slovak Act on Electronic Communications, which implements various EU law, including the ePrivacy Directive.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Privacy law is enforced by the Slovak DPO, which is entitled to inspect and assess the compliance of data processing operations with the GDPR and the DPA, and to issue orders and fines in cases where data protection laws have been violated. The Slovak DPO also publishes specific guidelines interpreting the GDPR and the DPA. The guidelines are not binding, but represent a useful source of information for entities processing personal data as well as for data subjects.

2 SCOPE

2.1 Which companies are subject to privacy law in Slovakia?

See the European Union chapter.

2.2 Does privacy law in Slovakia apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, privacy law applies outside the country:

(a) The GDPR applies to companies outside Slovakia in cases specified in Article 3 of the GDPR.

(b) Parts of the DPA apply to the processing of personal data of data subjects in the Slovak Republic by a controller or processor with headquarters, place of business, branch, establishment, or permanent residency not located in an EU Member state, where the processing of personal data is related to:

(i) the offering of goods or services, irrespective of whether payment is required, to a data subject in Slovak Republic; or

(ii) the monitoring of the behavior of data subjects, in so far as their behavior takes place within Slovak Republic.

For more information please see the European Union chapter.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Slovakia?

Personal data is legally defined in Article 4 of the GDPR. An identical definition is contained in Article 2 of the DPA.

For more information please see the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

Based on one of the GDPR opening clauses, the DPA 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

In accordance with Article 35(4) of the GDPR, the Slovak DPO 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Slovakia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in Slovakia? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

In addition to the GDPR, which regulates the processing of personal data, Slovak laws contain specific rules relating to the permissibility and the means of commercial communications. These rules are mainly contained in the Slovak Act on Electronic Communications and the Slovak Act on Advertising.

For the purposes of direct marketing, phone calls or use of automated call and communication systems without human intervention, facsimile, electronic mail, including short message service, to the subscriber or user are permitted only with his/her prior consent, which consent must be demonstrated. Prior consent of the recipient is not required in the case of direct marketing of similar goods and services to a recipient whose contact information was duly obtained by the same entrepreneur in connection with a previous sale of the goods or services.

The recipient of an email must be given the opportunity to refuse such use of contact information at any time. It is forbidden to send emails that do not show the identity and address of the sender to which the recipient may send a request to stop sending such messages.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter.

In addition to the privacy restrictions regarding tracking technologies contained in the GDPR, the Slovak Act on Electronic Communications rules that storing information, or gaining access to information stored, in a user's terminal equipment (not only personal data but all data which are being tracked) is permissible only if the user has given his/her consent, on the basis of clear and complete information about the purpose of such action. The use of appropriate settings of a web browser or other computer program shall also be deemed to be consent for this purpose. This does not prevent the technical storage of, or access to, data whose the sole purpose is to transmit or facilitate the transmission of the message over the network, nor where it is strictly necessary for the provision of the website service explicitly requested by the user. These rules, based on the ePrivacy Directive, are expected to be replaced soon by the ePrivacy Regulation.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

In addition to sanctions for breach of the GDPR, the DPA specifies sanctions for breach of those provisions of the DPA which are based on opening clauses of the GDPR. Finally, according to the DPA, the Slovak DPO may impose a procedural fine on anyone who does not cooperate during a data protection inspection.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Slovakia which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

From the prospective of privacy, the hottest topic is certainly the draft ePrivacy Regulation.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Slovakia?

At the time when the GDPR and the DPA became effective, the Slovak DPO unofficially suggested that it would not impose any fines for a period of 12 months. Since those 12 months have now passed, companies can no longer rely on the forbearance of the DPO.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Before the GDPR was adopted, Slovak legislation had already laid down detailed rules relating to the processing of personal data. However, few companies seemed to take these rules seriously. Compared to the sanctions that may be imposed under the GDPR, only symbolic penalties were imposed, so the area of personal data protection was paid relatively little attention. The adoption of the GDPR caused great hysteria in Slovakia, which culminated in May 2018, when, in particular, small and medium-sized companies started to look for last minute solutions to respond to GDPR requirements. Thanks to the GDPR, privacy has become an essential part of every business.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

There are still lot of uncertainties regarding personal data processing and privacy. This is because there is not yet sufficient case law, nor uniform guidelines for the interpretation of all GDPR clauses. Companies should therefore continue to monitor developments in the privacy landscape and continuously evaluate the compliance of their data processing operations with privacy laws, especially following interpretation by the supervisory authorities and courts. As far as online marketing is concerned, companies should also get ready for new rules under the ePrivacy Regulation.

SPAIN

1 PRIVACY LAW

1.1 How is privacy 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 are the highest (after the Spanish Constitution) in rank of legal regulations and require a special approval proceeding in the Parliament.

Article 18 of 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 Data Protection Directive 95/46/EC 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 Catalonian Authority on Data Protection; and the Council of Transparency and Data Protection of Andalusia. The region of Madrid established also its own regional agency for data protection in 2005 but it was closed in 2013.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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").

The GDPR is the main source for privacy regulation in Spain, as in the rest of EU Member States; however, due to the margin of adaptation left by the European legislator to the national authorities, the Spanish LOPD has developed some particularities, which can be summarized as follows:

(a) The LOPD introduces the concept of "data blocking", not present in the GDPR, but which the Spanish law defines as the "identification and reservation of the personal data, adopting technical and organizational measures, to prevent its processing, including its visualization, except for the provision of data to judges and courts, the Public Prosecutor's Office or competent Public Administrations, in particular the data protection authorities, for the requirement of possible responsibilities derived from the processing and only for the term of prescription of the same" (see, further, question 5.1);

(b) The minimum age at which any individual has capacity to give consent is fixed at 14 years;

(c) The LOPD specifies some additional entities and bodies which have the obligation to appoint a data protection officer ("DPO") (eg, educational entities, banks, insurance companies, sport federations, energy distribution companies, financial institutions, health and medical corporations, etc);

(d) Regarding the duty to inform, this must be presented through a layered (or granular) information system. The first layer must contain some basic minimum information, making the rest easily available for consultation on a second layer (see, further, question 3.3);

(e) There is special provision for personal data of deceased persons (see, further, question 3.1);

(f) There is legal presumption of lawful processing based on a legitimate interest or public interest in some specific situations (eg, processing of contact data in commercial transactions; video systems of surveillance; advertising exclusion systems; etc);

(g) The roles and duties of the data controller and the data processor are clarified (see question 4.1);

(h) Privacy violations are graded into three categories (minor, severe, very severe) and sanctions established in accordance with this classification (see question 10.1);

(i) The inclusion of a person on a "credit blacklist" is subject to specific and very strict conditions;

(j) Data processing for electoral purposes has a specific regulation (see question 11.1);

(k) Data processing agreements dated before May 25, 2018 will remain valid until their expiration. If the agreement has no expiration date, it will be in force until May 25, 2022; and

(l) A new catalogue of unfair competition practices relating the use of personal data has been enacted.

Although it was not included in the initial bill, the final text of the LOPD also includes 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.

On the other hand, 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 article 197 of the Spanish Criminal Code).

Another two regulations containing relevant provisions on privacy are the e-Commerce Law (Ley 34/2002), which implemented EC Directive 2000/31 on electronic and some of the provisions of EC Directive 2002/58 on Privacy and Electronic Communications; and the Law on General Telecommunications (Ley 9/2014).

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 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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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. In 2018 and 2019 the Agency published the following guides:

(a) Guide about the use of cookies;

(b) Guide about the privacy by design;

(c) Practical guides about performance of risk analysis and data protection impact assessments ("DPIA"s);

(d) Guide about the use of video surveillance and biometric systems;

(e) Guide for notification of security breaches;

(f) Guide about the right of information; and

(g) other sectorial guides (eg, for Public Administrations, education centers, etc).

In addition, the AEPD provides a help tool, called Facilita. This tool helps companies and professionals who process low-risk personal data to comply with the new GDPR. It takes the form of an online questionnaire taking a maximum of 20 minutes to complete, which companies and professionals can use; firstly, to verify, by means of a series of questions, that the data they process can be considered low risk and, secondly, to obtain the essential documents required to enable 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 the professional privacy enterprises and to the entities that hire their services.

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 his 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".

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.

There is no self-regulatory system relating to disputes about privacy; however, Autocontrol, which is 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.

2 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Spain?

Personal data is legally defined in Article 4(1) of 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The Spanish LOPD does not add new categories of sensitive data to those listed in the GDPR; however it excludes the exception granted by Article 9(2)(a) of 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

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.

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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The Spanish LOPD clarifies the roles established by GDPR. In particular, a "controller" is the person who, in his 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 will 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union Chapter.

The AEPD has published a list of situations in which risk impact assessments are mandatory; and also a list of situations and actions excluded from this obligation (see question 11.3).

Another difference in the Spanish privacy legal framework relates to the advertising exclusion systems (eg, "Listas Robinson"), regulated specifically in Article 23 of 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 granted previously his/her consent to that particular commercial communication.

The appointment of a DPO is compulsory and must be communicated to the AEPD in certain cases, including entities carrying out advertising and commercial research activities based on the data subjects' preferences or carrying out data subjects' profiling actions.

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.

"Data blocking", is one of legal innovations of the Spanish LOPD (see question 1.2(a)). 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Spain? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

Providers of telecommunication services have special duties which are regulated by the General Telecommunication Act.

The AEPD has published a guide about data security and breach which is available on its website.

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.

6.2 How are data breaches regulated in Spain? What are the requirements for responding to data breaches?

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. In Spain, the notification can be made by the controller using standardized forms through an on-line system created by the Agency for this purpose (certified electronic signature is required): https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

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.

(b) 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.

(c) 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.

(d) The right of access is considered fulfilled if the controller offers the data subject means that permanently guarantees remote, direct and secure access to his/her personal data.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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 above). The following are the most relevant:

(a) When consent is sought for the processing of the data for several purposes, it will be 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) Sending unsolicited digital commercial communications is only allowable if there has been a previous commercial/contractual relationship with the data subject, or if express consent has been granted (see question 5.1). An opt-out possibility must be offered in every communication.

(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) See question 5.1 about advertising exclusion systems.

(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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is specific guidance about cookies issued by the AEPD in November 2019. Express and positive consent is required in application of GDPR rules; however, the option "if you continue browsing you grant your consent to our use of cookies" is permitted under certain conditions.

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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

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 about data transfers must be complied with.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs may be considered to be a commercial relationship, which entitles the controller to process data on the basis of this consent (agreement) and allows him 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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Although 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: Article 72 of the LOPD lists of violations considered very serious offenses (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: Article 73 provides a list of violations considered serious offenses (eg, procession 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: Article 74 lists violations considered as minor infringements, such as 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 equal or under 40,000 euros have a limitation period of 1 year; sanctions between 40,001 and 300,000 euros have a limitation of 2 years; and sanctions over 300,001 euros have a limitation period of 3 years.

10.2 Do individuals have a private right of action? What are the potential remedies?

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 stating, eg, the controller's obligation to inform all employees about the system.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Spain which affect privacy?

The new LOPD modified the Law of the General Electoral System introducing, through article 58 bis, 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 (no application of e-Commerce Regulation).

This provision caused huge public concern and was challenged before the Constitutional Court, which declared on May 2019 that this modification of the Electoral Act was contrary to the Constitution and void.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The protection of minors is, among others, a very relevant issue for the local authority at this moment. A specific digital tool has been implemented for this purpose (AseguraTIC).

AEPD is also warning about some companies which are offering adaptation services and legal advice about the GDPR for zero or very low cost.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Spain?

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

(www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf). 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, eg:

(a) the profiling or assessment of subjects;

(b) the observation, monitoring, geolocation or control of the data subject in a systematic and exhaustive manner;

(c) the use of special categories of personal data, data related to criminal convictions or data that allow to determine the economic solvency;

(d) the use of biometric data to uniquely identify a person;

(e) the use of genetic data; or

(f) 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.

Previously, the AEPD had published another list containing those processing activities for which it is not mandatory to carry out an impact assessment (www.aepd.es/media/guias/ListasDPIA-35.5l.pdf).

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the 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.

SWEDEN

1 PRIVACY LAW

1.1 How is privacy 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 European Union law, also govern privacy. Furthermore, the data protection authority has issued guidelines which, although non-binding, assist practitioners to comply with privacy issues.

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 with regard to 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 entered into force.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The European General Data Protection Regulation ("GDPR") is the primary source governing privacy in Sweden.

Aside from the GDPR, Sweden has adopted the Data Protection Act, supplemented by the Data Protection Ordinance (2018:219). The Data Protection Act is subsidiary law, meaning that its provisions do not apply if there is specific legislation governing the same matter.

In addition, there are so called "Registry Acts" governing specific aspects of register-keeping involving personal data. To mention a few, the Registry Acts govern fields such as law enforcement, financial activities, and healthcare. In general, the Registry Acts are directed at public authorities, but in some cases, the Registry Acts also apply to private entities, depending on what activities the relevant controller or processor is involved in.

The Swedish Electronic Communication Act ("LEK"), often referred to as the "Cookie Law", is also relevant to privacy. The LEK implemented the ePrivacy Directive 2002/58/EC.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Sweden has appointed the Swedish Data Protection Authority ("SDPA") as its supervisory authority for data protection. The SDPA is therefore the supervisory authority of the GDPR, the Data Protection Act, the Data Protection Ordinance as well as a number of other laws (eg, some of the Registry Acts).

The scope of the SDPA's mission follows from GDPR Article 51. Aside from the provisions of GDPR Article 51, the role of the SDPA is further explained in the Swedish Regulation with Instructions for the SDPA (2007:975). This Regulation states that the SDPA's mission is to ensure that fundamental human rights are protected in connection with the processing of personal data, to facilitate the free flow of personal data within the EU, and to ensure that good practices are observed in credit and debt collection operations.

The powers of the SDPA follows from GDPR Article 58 and include, inter alia, the authority to order the controller and the processor to provide any information it requires for the performance of its tasks, and to carry out investigations in the form of data protection audits. Upon violation of data protection law, the SDPA is authorized to issue warnings, injunctions, and impose administrative sanctions in line with the GDPR.

Sweden has no self-regulatory bodies enforcing privacy law.

2 SCOPE

2.1 Which companies are subject to privacy law in Sweden?

See the European Union chapter with regard to which companies are subject to the GDPR.

Chapter 1 Section 5 of the Data Protection Act set out its scope of application, making the Act apply to:

(a) processing of personal data conducted from a controllers'/processor's place of establishment in Sweden;

(b) processing of personal data conducted by a controller not established in Sweden, but in a location where Swedish law applies according to international law; or

(c) processing of personal data carried out by a controller/processor established in a third state, if the processing concerns data subjects located in Sweden, and if such processing is connected to either the offering of goods or services to such data subjects, or the monitoring of such data subjects' behavior in Sweden.

The territorial scope of the Data Protection Act is rather similar to the wording of GDPR Article 3, although with Sweden as the territorial reference point instead of the European Union. As is apparent from the territorial scope of the Data Protection Act, a company established outside of Sweden could still have to comply with the provisions of the Act.

The Registry Acts have different scopes of application, each being adapted to its relevant field of business.

2.2 Does privacy law in Sweden apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 INFORMATION

3.1 How is personal information/personal data defined in Sweden?

The Data Protection Act and the Registry Acts refer to the definitions provided by the GDPR. This means that the Swedish definition of "personal data" is identical to the definition provided by the GDPR Article 4(1). For a detailed description of the definition of "personal data", see the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

In Sweden, special categories of personal data and sensitive personal data are defined as provided by the GDPR. See the European Union chapter.

Chapter 3 of the Data Protection Act sets out provisions relevant to the processing of certain categories of sensitive personal data. In general, Chapter 3 of the Data Protection Act provides a number of exceptions to the general prohibition on processing sensitive personal data set out by GDPR Article 9(1). The 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 law, 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. Processing of personal identification numbers is not significantly controversial in Sweden, in comparison to other Member States of the European Union. Personal identification numbers are, nevertheless, considered as a special category of personal data under Swedish law. This follows from Chapter 3 Section 10 of the Data Protection Act. According to the Data Protection Act, personal identification numbers may be processed without the data subject's consent only if such processing is justifiable, taking into account:

(a) the purpose of the processing,

(b) the importance of a safe identification, or

(c) any other remarkable purpose.

With regard to children's personal data, Chapter 2 Section 4 of the Data Protection Act sets out that, when offering information society services to a child domiciled in Sweden, processing of personal data of such child shall be lawful based on the child's consent, but only if the child is at least 13 years. If the child is less than 13 years, processing of the child's personal data is lawful only if, and to the extent that, consent is given or authorized by the holder of parental responsibility. Thus, Sweden applies the lowest age limit for the processing of children's personal data permitted under the GDPR.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

The SDPA has published non-binding guidelines on the key principles of the GDPR. These guidelines set out a number of measures that companies should take in order for their processing of personal data to be lawful. The guidelines set out the following points as key (though include others):

(a) Inform the data subjects that their personal data is collected;

(b) Decide in advance what the personal data shall be used for, and do not use the personal data for other purposes;

(c) Do not collect more personal data than needed to fulfil the purpose for which the personal data was collected;

(d) Ensure that the personal data are correct and updated;

(e) Protect the personal data processed; and

(f) Erase personal data that is no longer necessary to process.

The SDPA has also included a checklist for companies to follow in order to be compliant with the GDPR.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Sweden? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union Chapter.

The SDPA has stated that it will not provide detailed instructions for controllers or processors on what security measures to take in order to comply with the security standards of the GDPR. However, it has provided non-binding guidelines on what security measures companies can take in order to fulfil the security standards of the GDPR. These guidelines should be treated as recommendations, rather than an exact statement of what is required in order to be compliant with the GDPR.

In its guidelines, the SDPA states:

(a) the controller (or, as applicable, the processor) must be aware of what personal data they process.

(b) transparency with regard to the processing of personal data (eg, communication with data subjects via a privacy policy) is key.

(c) the importance of following the rigorous requirements with regard to keeping of documentation, set out by the GDPR, and of continuously conducting impact assessments and performing vulnerability tests.

6.2 How are data breaches regulated in Sweden? What are the requirements for responding to data breaches?

See the European Union chapter.

The LEK contains requirements for providers of public electronic communications services to notify the supervisory authority about privacy incidents. The Swedish Post and Telecom Authority ("PTS") is the supervisory authority with regard to the LEK. Chapter 6 Section 1 of the LEK defines a "privacy incident" as an event leading to unintentional or unauthorized destruction, loss or alteration, or unauthorized disclosure of or unauthorized access to information processed when offering public electronic communication services. If a privacy incident occurs, it must be reported to PTS. Under certain circumstances, for instance if the privacy incident may have negative effects for the users or subscribers, or on PTS' request, users or subscribers must also be notified about the privacy incident.

PTS has identified that problems may arise in determining whether an incident should be reported as a privacy incident, and thus to the PTS, or as a personal data breach (as defined by the GDPR), and thus to the SDPA. Therefore, PTS has issued non-binding guidelines to help in making this distinction. As a general rule, an incident (if considered a personal data breach that must be reported) should be reported to the SDPA only if it should not be reported to the PTS pursuant to the provisions of LEK, because of LEK's character as a *lex specialis* in relation to GDPR.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

The Data Protection Act set out a number of limitations to data subjects' rights under GDPR. For instance, GDPR Article 15 does not apply to personal data that has not had its final configuration when the data subject submitted his/her request. This means that a controller is not obliged to include concepts, drafts or similar when fulfilling its obligations pursuant to GDPR Article 15. This exception comes with limitations, eg:

(a) if the personal data in question has been submitted to a third party,

(b) if it is processed for archive purposes of public interest or statistical purposes, or

(c) if the personal data has been processed for more than one year even though it has not been finalized.

In addition, the exception does not apply to texts intended to be changed or finalized on a continuous basis.

In addition, GDPR Articles 13-15 do not apply to personal data that the controller cannot disclose according to EU or Swedish Law, such as the Public Access to Information and Secrecy Act. This follows from Chapter 5 Section 1 of the Data Protection Act.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

The Swedish Marketing Practices Act sets out provisions relevant for marketing via email, fax or telephone. According to Section 19 of the Marketing Practices Act, 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 his/her prior consent. However, the Marketing Practices 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.

With regard to processing of personal data for direct marketing purposes, Swedish case law (although based on the repealed Personal Data Act) states that traders may send marketing messages to natural persons if there is an active relation between the organization and the natural person. Also following from case law, organizations may, at least as a general rule, 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 SDPA has stated that a retailer selling sporting gear may keep information about its customers in order to perform direct marketing measures aimed at the data subject with regard to the retailer's similar products.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter with regard to 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.

Chapter 6 Section 18 of the LEK states that 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 they have given their 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 or the 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. However, the government bill which provides guidance to the LEK states that consent to the use of cookies may be given by the web-browser settings (eg, allowing cookies in the browser settings), although, beyond this, the government bill is silent on the matter of how a valid consent should be given under the LEK.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Sweden which affect privacy?

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 Are there any hot topics or laws on the horizon that companies need to know?

As is the case in many other Member States, a hot topic in Sweden is the draft ePrivacy Regulation. 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 cautions around processing personal information/personal data in Sweden?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

The SDPA has started to become more active in terms of issuing fines and conducting audits. During the first period after the entering into force of the GDPR, the SDPA was somewhat reluctant to issue fines as well as to perform audits. It is probable that the development of the SDPA will continue, which could mean that we will see an increasing number of fines and audits in the years to come.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

In Sweden, as has been mentioned in question 12.1, we may see a more active SDPA in exercising its powers. Consequently, we may see more guiding judgments on complex privacy issues in the years to come.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

One of the challenges is to connect new technology, as well as companies with businesses involving such technology, to the privacy landscape.

GHANA

1 PRIVACY LAW

1.1 How is privacy regulated in Ghana?

Privacy is regulated by Acts of Parliament and by the 1992 Constitution of the Republic of Ghana.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) The 1992 Constitution of Ghana contains principles that recognize and protect the right to privacy of its citizens. Article 18(2) of the 1992 Constitution of Ghana 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 and or protection of others.

(b) Act 843, the Data Protection Act 2012 ("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 other laws which are sector-specific and impact data protection/privacy in Ghana. These include:

(c) Act 775, the Electronic Communications Act 2008 (as amended by Act 786, the Electronic Communications (Amendment) Act) ("Electronic Communications Act"); as well as

(d) the Electronic Communications Regulations 2011 (LI 1991) ("Electronic Communications Regulations").

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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").

2 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 processors are required to register with the DPC. Those not incorporated in Ghana must register as an external company.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Ghana?

The Data Protection Act defines "personal data" as data about an individual who 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The Data Protection Act defines "special personal data" as personal data which consists of information that relates to:

(a) the race, colour, 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

(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.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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.

(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 controller bears the 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The Data Protection Act places an obligation on data controllers to register with the DPC before collecting or processing personal data, whether the entity is located in or outside of Ghana.

The DPC, in this instance, is a privacy authority. Registration with the DPC is renewable every two years. The Data Protection Act provides for appointment of privacy officers and stipulates that personal data should not be retained for a period longer than is necessary to achieve the purpose for which the data was gathered.

In addition, the data controller must take steps to secure the integrity of personal data in its possession, and adopt measures to prevent, loss or unauthorised access to the data.

Furthermore, a data protection supervisor must be appointed, whose details must be entered at the point of registration with the DPC.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Ghana? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Section 28 of the Data Protection Act provides for the securities measures for protecting data. The data controller must adopt general practices and procedures, as well as specific industry rules and regulations, in order to secure the personal data it has gathered.

6.2 How are data breaches regulated in Ghana? What are the requirements for responding to data breaches?

The data controller must notify the DPC and the data subject of the unauthorised 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 unauthorised person, and take steps to ensure the restoration of the integrity of the information systems.

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 200 penalty units (approx GHC 2,400 (US $432)), or a term of imprisonment of not more than two years, or both.

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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The data subject can refuse to consent to his/her data being processed and data must be sourced directly from the data subject. It may be sourced indirectly only if it is information already in the public domain or information for prosecution of an offence, conduct of a trial in court, or enforcement of a law which imposes pecuniary penalties or concerns revenue collection.

The data subject also has the right to complain in writing to the DPC where his/her rights are being breached under the Data Protection Act.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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. Under the Regulations, persons other than the sender or intended recipient who steal, intercept, alter, divert or unlawfully disclose transmitted messages or data commit an offense and are liable on summary conviction to a fine of not more than 500 penalty units (approx GHC 6,000 (US $1,080)), or a term of imprisonment of not more than 5 years, or both.

Moreover, operators must employ international best practices in the industry to promote privacy, secrecy and security of communication and personal accounts/data related to subscribers. Anyone who breaches this is liable to a fine of not more than 500 penalty units, or a fine indicated in the person's licence where higher.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The Data Protection Act is silent on tracking technology.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The Electronic Communications Regulations provide that a person who wishes to send unsolicited communications for direct marketing by a 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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The Data Protection Act provides that the data subject's prior written consent must be sought and obtained before the data can be obtained or provided for the purposes of direct marketing. It also gives the data subject the right to give notice in writing to the data controller that it should not process his personal data for the purpose of direct marketing.

8.5 Are there specific privacy rules governing data brokers?

The Data Protection Act is silent on data brokers.

8.6 How is social media regulated from a privacy perspective?

Though the Data Protection Act does not specifically provide for privacy with respect to social media, Section 40(4) states that direct marketing includes the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programmes and promotions are regulated by the Gaming Commission which is created and regulated by the Gaming Act 2006 (Act 721).

This Act sets guidelines for running promotional and loyalty programmes 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 licenced 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 GHC 3,000–12,000 (US $540–2,160)).

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Section 25 of the Data Protection Act states:

"(1) Where a data controller holds personal data collected in connection with a specific purpose, further processing of the personal data shall be for that specific purpose.

(2) A person who processes data shall take into account:

(a) the relationship between the purpose of the intended further processing and the purpose for which the data was collected,

(b) the nature of the data concerned,

(c) the manner in which the data has been collected,

(d) the consequences that the further processing is likely to have for the data subject, and

(e) the contractual rights and obligations between the data subject and the person who processes the data.

(3) The further processing of data is considered to be compatible with the purpose of collection where:

(a) the data subject consents to the further processing of the information,

(b) the data is publicly available or has been made public by the person concerned…"

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Companies should be mindful of Section 25 of the Data Protection Act, as well as the need to also notify the data subject and obtain his/her consent where needed before utilising the data gathered.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 GHC 3,000 (US $540)), or a term of imprisonment of 2 years, or both;

(b) for purchasing or knowingly obtaining or disclosing personal data to another person: a fine of not more than 250 penalty units, or a term of imprisonment of 2 years, or both;

(c) for sale of personal data: a fine of not more than 2,500 penalty units (approx GHC 30,000 (US $5,400) or a term of imprisonment of not more than 5 years or both; and

(d) for all offenses for which the Act does not specify the penalty: a fine of not more than 5,000 penalty units (approx GHC 60,000 (US $10,800) or a term of imprisonment of not more than 10 years, or both.

10.2 Do individuals have a private right of action? What are the potential remedies?

The 1992 Constitution of Ghana contains principles that recognize and protect the right to privacy of its citizens.

Article 18(2) of the Constitution 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.

Section 39(1) of 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."

Furthermore, Section 43 of the Data Protection Act provides that 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Ghana which affect privacy?

We are not aware that any such rules exist at this time.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

There is a Bill proposed for the regulation of Advertising in Ghana. The Bill is currently before Parliament. Once passed, it will be the major law regulating advertising in Ghana.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Ghana?

Personal data processed by an individual for the purpose of that individual's personal, family or household affairs is exempted from the data protection principles, as is personal data which consists of a reference given in confidence by the data controller for the purpose of education, training, employment, or appointment to an office of the data subject, or provision of any service by the data subject.

The processing of personal data is also exempt from the provisions of the Data Protection Act if it is for the purpose of public order, safety, morality or national security.

The Act also does not apply to the processing of personal data for the protection of members of the public against loss or malpractice in the provision of banking, insurance, investment or other financial services, or against dishonesty in the provision of professional services, or where the processing is for the discharge of a function conferred under an enactment on the Parliament of the government or for health care or disease prevention etc.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The introduction of the Data Protection Act has created the DPC, which is actively regulating the collation, use and dissemination of data in Ghana. Thus, people are more aware of the issues surrounding data protection and privacy in Ghana. Also, the existence of a regulator which can prosecute offenders serves as a deterrent for violation of privacy and tends to reduce such incidences.

12.2 What do you envision the privacy landscape will look like in 5 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.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

A major challenge will be securing data that has been gathered from hackers or unauthorised users, due to the advent of technology.

GUATEMALA

1 PRIVACY LAW

1.1 How is privacy regulated in Guatemala?

Currently, Guatemala lacks data privacy specific legislation; therefore, there are no regulations detailing matters such as how data can be collected, legally processed, transferred and enforced. However, there is a specific law regarding access to public information, which, among other matters, covers personal data contained in public archives or records.

Instead, 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.

The Public Information Access Law, Decree 57-2008 of Congress, contains a specific chapter "Habeas Data", defining this as the guarantee that every person has to exercise the right to know what is recorded about him/her in public records, and the purpose for which such data is used, as well to exercise the right to protect, update, amend or rectify such data. Decree 57-2008 applies to public entities or entities that manage public funds and/or have competence in public administration.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The following are the key laws regulating privacy in Guatemala:

(a) Political Constitution of the Republic of Guatemala;

(b) Public Information Access Law, Decree 57-2008 of Congress; and

(c) Criminal Code, Decree 17-73 of Congress.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Privacy is enforced through tribunals via constitutional actions, in particular the "amparo" action. Depending on the infringement, there are administrative, civil and criminal procedures that could be initiated, since, under the current legal framework, there is no privacy regulator nor 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 SCOPE

2.1 Which companies are subject to privacy law in Guatemala?

All companies are subject to 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, lack of specific regulations makes for a domestic private environment that fails to provide any guidance as to specific practices, management and protection of personal data. Other than the provisions contained in Decree 57-2008, under the "Habeas Data" chapter, there are few applicable regulations.

2.2 Does privacy law in Guatemala apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Law and jurisprudence apply territorially (that is, locally), but apply to both national and non-national companies operating in Guatemala.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Guatemala?

Under Decree 57-2008, "personal information"/"personal data" is any information related to an identified or identifiable natural person.

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 his/her identity (eg, from an identification number to, among others, physical, social, cultural, and economic characteristics of such person).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The only law that provides for such a classification is Decree 57-2008, which distinguishes between personal data and sensitive information. "Sensitive information" includes:

(a) physical characteristics;

(b) moral characteristics;

(c) facts or circumstances of one's private life or activities, such as habits, racial origin, ethnicity, political ideologies and opinions, beliefs or religious convictions;

(d) state of physical or mental health;

(e) sexual orientation; and

(f) moral and family situations and other intimate issues of similar nature.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Following the interpretation that the Constitutional Court has given to the matter, the principles to be considered by any company for processing personal information are:

(a) to obtain the explicit consent of the data subject;

(b) not to commercialize the data without authorization from the data subject;

(c) to guarantee to the data subject:

(i) the right to consult his/her data,

(ii) the right to correct his/her data,

(iii) confidentiality, unless the data subject has given express authorization for the data to be used in specific ways.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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 it contractually, considering best practices.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Lack of a specific law means that a list of key obligations cannot be given. However, decisions from the Constitutional Court refer to principles to be considered by any company for processing personal information, namely:

(a) to obtain the explicit consent of the data subject;

(b) not to commercialize the data without authorization from the data subject;

(c) to guarantee to the data subject:

(i) the right to consult his/her data,

(ii) the right to correct his/her data,

(iii) confidentiality, unless the data subject has given express authorization for the data to be used in specific ways.

As regards personal data in advertising, this cannot be used without the express authorization of the data subject.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Guatemala? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Under the section titled “Habeas Data” of Decree 57-2008, those holding the personal data of others are obliged to adopt proper measures to guarantee the security, confidentiality of personal data and avoid its alteration, loss and unauthorized use.

Personal data security in general is subject to civil law, particularly as regards any breach of a data recipient's responsibilities and any damages that could result from it; therefore, companies should consider contractual wording in order to define the scope of their liabilities.

6.2 How are data breaches regulated in Guatemala? What are the requirements for responding to data breaches?

There is no specific regulation to address data breaches; this means there are no mandatory requirements or procedures to comply with in response to the unauthorized use of the data by a data recipient, or to inform the data recipient of data breaches. Notwithstanding the above, it is highly recommendable for any company to set up a protocol to be implemented in response to data breaches.

The Criminal Code regulates specific crimes regarding data security breaches, such as:

(a) deletion of databases,

(b) creation of prohibited records,

(c) unauthorized alteration of the information contained in the databases and

(d) unauthorized use of data.

Decree 57-2008 also regulates specific crimes regarding data security breaches, namely:

(e) the unauthorized commercialization of personal data,

(f) the unauthorized alteration or destruction of information contained in archives,

(g) the unjustified retention of information and

(h) the disclosure of confidential information.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The Constitutional Court of Guatemala has established that the rights of the individual in relation to his/her personal data are:

(a) the right to consult his/her data;

(b) the right to correct his/her 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 interested party; and

(e) the right that commercialization of his/her personal data be done only with his/her express authorization.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications are not specifically regulated in Guatemala. Therefore, the content of communications should observe the different regulations that are disseminated in different laws. Although currently this is not a regulated practice, companies should at least consider that individuals should have the right to request the cessation of email marketing and push notifications.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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 how information and activity online is tracked, registered or controlled.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

These kinds of publicity are not specifically regulated. Nevertheless, the Constitutional Court decisions makes it clear that giving of information and obtaining consent are key. The main principles that companies should observe are:

(a) to obtain explicit consent;

(b) not to commercialize the data without authorization from the data subject;

(c) to guarantee to the data subject:

  (i) the right to consult his/her data,

  (ii) the right to correct his/her data, and

  (iii) confidentiality, unless there is express authorization from the data subject for the data to be used in specific ways.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

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 the abovesaid, the other principles also apply, meaning that all data subjects have the right:

(a) to know the content of his/her personal data; and

(b) to have guaranteed the right to consult and correct his/her data and the right of confidentiality in the customer matching process.

8.5 Are there specific privacy rules governing data brokers?

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 requirements:

(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:

(i) the data broker to determine the veracity of the data;

(ii) the data broker to be able to update the data under its solely responsibility; and

(iii) the data subject to have the right to rectify the data.

8.6 How is social media regulated from a privacy perspective?

There are no specific laws regulating social media. Nonetheless, the Constitutional Court has stated considerations relating to data privacy, particularly considerations as to data privacy and right of intimacy and explicit consent. In this regard, the Court has stated that:

(a) The collection of any personal data must have a defined purpose, and data 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) Those who register and use personal information must implement adequate mechanisms of control for:

(i) the recipient to determine the veracity of the data;

(ii) the recipient to be able to update the data under its solely responsibility; and

(iii) the data subject to have the right to rectify the data.

Additionally, companies or any person that interacts with personal data in social media must be aware that slander is punished under the Criminal Code.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs and promotions are not specifically regulated. However, companies must not only provide proper and clear information when collecting data and state the uses to which they intend to put it, but also obtain an explicit consent from the data subject.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The requirements that must be observed for data transfer are the same as those that data brokers or data recipients must observe. See, eg, question 8.5.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Companies must observe the requirements imposed by the Constitutional Court (see, eg, question 8.5). In addition, data recipients that transfer data must secure, in any way (ie, a contract), that the entity receiving the data uses it subject to the same restraints.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

(a) The Criminal Code stipulates the following penalties:

(i) Destruction of database: Prison term of between 6 months and 4 years and a fine of Q200.00–Q2,000.00.

(ii) Creation of prohibited records: Prison term of between 6 months and 4 years and a fine of Q200.00–Q1,000.00.

(iii) Unauthorized alteration of information contained in databases: Prison term of between 1 and 5 years and a fine of Q500.00–Q3,000.00.

(iv) Unauthorized use of data: Prison term of between 6 months and 2 years and a fine of Q200.00–Q1,000.00.

(v) Slander: Prison term of between 2 and 5 years.

(b) As mentioned, Decree 57-2008 of Congress also contains certain crimes for which sanctions are:

(i) Unauthorized commercialization of personal data: Prison term of between 5 and 8 years and a fine of Q50,000.00–Q100,000.00.

(ii) Alteration or destruction of information contained in archives: Prison term of between 5 and 8 years and a fine of Q50,000.00–Q100,000.00.

(iii) Unjustified retention of information: Prison term of between 1 and 3 years and disqualification for twice the prison time and a fine of Q10,000.00–Q50,000.00.

(iv) Disclosure of confidential information: Prison term of between 5 and 8 years and disqualification for twice the prison time and a fine of Q50,000.00–Q100,000.00.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes, the affected individuals have the "amparo" action. The potential remedy is to stop the action that is infringing their rights.

Individuals also have possibility of bringing a criminal action for the specific crimes contained in the Criminal Code and Decree 57-2008 (see question 10.1). Another possibility could be to bring a civil action, which might be exercised as a consequence of the criminal procedures or exercised independently. In either case, the potential remedy is damages.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Guatemala which affect privacy?

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 certain cases, as these were applied to specific cases that all followed "amparo" actions in which particular facts were observed. Therefore, it is essential that best practices, protocols and contractual wording between parties to build and protect data privacy are drawn up. Guatemala is still at an early stage in privacy matters, but we are optimistic that a data protection law will be enacted by Congress in the near future.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Companies need to be aware that the draft bill regarding personal data protection may be enacted. This draft bill contains, among other things:

(a) a definition of personal data and sensitive personal data,

(b) the principles for the treatment of personal data,

(c) the rights of the data subject,

(d) the scope of consent,

(e) the definition and obligations of the data recipient,

(f) the conditions for the transfer and deletion of the data,

(g) the regulatory bodies, procedures and sanctions.

In brief, this draft bill will give clarity about the matters that only the Constitutional Court has pronounced nowadays.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Guatemala?

We have no specific additional advice, but, would reiterate, lack of legislation does not imply freedom of action; thus, appropriate notices, information and explicit consent is advisable for companies in order to properly document manage data of third parties and share or transfer it to others. Work based on best practices is highly recommended.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

This matter has taken on more and more relevance with time. Individuals have become more aware of the value of their personal data, and of their right to exercise and demand privacy. The use of particular data brokers had led to situations that propelled individuals to seek protection via "amparo" action. In this sense, the Constitutional Court has recognized the right to data privacy, right of intimacy and explicit consent and has stipulated fixed requirements that data recipients must observe (see earlier questions).

12.2 What do you envision the privacy landscape will look like in 5 years?

We envision that the Constitutional Court will issue an exhortative decision, in which it encourages Congress to issue a specific law on data privacy. Such specific law could be the draft bill that has been before Congress since 2009.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Companies must properly monitor how data is obtained and managed in order to secure a balance in the legal system between a lack of a specific law and the implementation of reasonable and appropriate documents for the use of the personal data, relying on best practices.

Additionally, they will always have to double check agreements that they make with other companies, to ensure that these other companies observe the same parameters of protection and security.

HONDURAS

1 PRIVACY LAW

1.1 How is privacy 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.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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 SCOPE

2.1 Which companies are subject to privacy law in Honduras?

As Consumer Protection is the main regulatory framework, all companies who sell products directly to end-consumers are subject to privacy law.

2.2 Does privacy law in Honduras apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The Honduran regulatory framework does not make a distinction on what can be considered sensitive information.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

There are no obligations on the handling of information of clients/consumers. What Honduran law regulates is the period of time for which companies must maintain information on ad campaigns in their files and have hot-lines for consumer complaints for their ads. There are also regulations forbidding advertising that targets competition.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Honduras? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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. Currently only two companies are certified to provide this service in Honduras.

6.2 How are data breaches regulated in Honduras? What are the requirements for responding to data breaches?

Data breaches are not yet regulated.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The Honduran Constitution recognizes that 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications are not regulated from a privacy perspective. Financial system laws only regulate the time periods during which companies can contact clients.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Tracking technologies are not regulated from a privacy perspective.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertising and behavioral advertising are not regulated from a privacy perspective.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The sharing of data with third parties for customer matching is not regulated.

8.5 Are there specific privacy rules governing data brokers?

No.

8.6 How is social media regulated from a privacy perspective?

Social media is not regulated from a privacy perspective.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Companies are allowed to collect consumer information during promotions or loyalty programs; however, there are no regulations how this information is to be stored.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Group companies can transfer data freely amongst themselves. There are no regulations on data transfer outside the country.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

No.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 US $400 to US $4,000,000, depending on the severity and recurrence of the breach.

10.2 Do individuals have a private right of action? What are the potential remedies?

Everyone has the right to access information about themselves or their assets in an expeditious and free manner, whether it is contained in public or private databases, and has the right, if necessary, to update, rectify and/or amend it.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Honduras which affect privacy?

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 Are there any hot topics or laws on the horizon that companies need to know?

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. Congress is expected to pick it back up in 2020. See question 11.3.

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 cautions around processing personal information/personal data in Honduras?

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 you observed over the past few years? In your opinion, what propelled/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 do you envision the privacy landscape will look like in 5 years?

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.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

There aren't many challenges now, as there is little to no regulation. Challenges are going to come to companies accustomed to the current landscape, which will have to adapt to the implementation of new regulation in the country.

HONG KONG

1 PRIVACY LAW

1.1 How is privacy regulated in Hong Kong?

Privacy per se is not protected in Hong Kong. The tort of "breach of privacy" established by the High Court of England and Wales in the case of Mosley v News of the World Newspaper in 2008 may possibly be taken as a persuasive authority for a similar action in the Hong Kong courts — something which has not yet happened.

Article 17 of the International Covenant for Protection of Rights was imposed on the Hong Kong SAR by Article 39 of the Basic Law of China for Hong Kong and establishes a positive duty to protect the right of privacy. It is clearly difficult, if not impossible, to define the parameters of the right of privacy in precise terms, but it is clear that the common law does recognize the intrusion upon privacy of a person who can show the commission of an established tort such as breach of confidence. Here the victim has a cause of action which can effectively operate to set up a separate and conjoined right established on the same facts, but which is subsumed to constitute the tort of breach of confidence which is recognized by the courts.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

There are no laws in Hong Kong regulating privacy per se. The essential foundation of Hong Kong's social structure has always been total freedom of expression and it has always been an anathema to seek to impose control on this.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

There is no statutory machinery to enforce privacy.

2 SCOPE

2.1 Which companies are subject to privacy law in Hong Kong?

Neither companies nor individuals are subject to privacy law per se.

2.2 Does privacy law in Hong Kong apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

There is no privacy law in Hong Kong which applies to companies outside Hong Kong.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Hong Kong?

The Personal Data (Privacy) Ordinance ("PDPO"), which was enacted in 1996, is the first statutory law in Hong Kong aimed at and protecting the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith.

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 (the way you walk).

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Biometric, health, video, geo-location and financial data and data and related to children represent the categories of personal data subject to the protection of the PDPO.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

There are six data protection principles ("DPPs") scheduled to the PDPO which are:

(a) DPP1: purpose and manner of collection;

(b) DPP2: accuracy and duration of retention (see further question 6.1(a));

(c) DPP3: use of data;

(d) DPP4: data security (see further question 6.1(b));

(e) DPP5: openness and transparency (see further question 5.1(a)); and

(f) DPP6: access and correction (see further question 7.1(b)).

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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 but the PDPO requires that the data user must enter into a stringent 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

(a) 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. 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.

(b) 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. Accordingly, there is currently no requirement in Hong Kong to appoint a privacy officer, nor to register with the Commissioner, nor to conduct risk impact assessments, although voluntary compliance with such precepts would likely merit commendation by the Commissioner.

(c) The duty of keeping secure records of data processing operations is imposed by DPP4 (see question 6.1(b)).

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Hong Kong? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

(a) Under DPP2, all practicable steps must be taken by the data user to ensure that personal data is accurate having regard to the use 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 or is to be used and, as stated in question 4.1 above, 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 and in this principle "data processor" means a person who:

(i) processes personal data on behalf of another person; and

(ii) does not process the data for any of the person's own purposes.

(b) DPP4 requires that the data user shall 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 the kind of data, the physical location of storage of the data, security measures incorporated into any equipment of storage of the data and 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 behalf of the data user, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

6.2 How are data breaches regulated in Hong Kong? What are the requirements for responding to data breaches?

An individual, or a relevant person on behalf of an individual, may make a complaint to the Personal Data Privacy Commissioner ("the Commissioner") about an act or practice:

(a) specified in the complaint; and

(b) which:

(i) has been done or engaged in or is being done or engaged in, as the case may be, by a data user specified in the complaint;

(ii) relates to personal data of which the individual is or, in any case in which the data user is relying upon an exemption under the Ordinance, may be, the data subject; and

(iii) may be a contravention of a requirement under the PDPO.

A complaint must be in writing in Chinese or English, but the Commissioner is empowered to accept a complaint in another form.

Before the Commissioner carries out an investigation into the complaint, he must serve notice in writing on the relevant data user informing the data user of his intention to carry out the inspection or investigation as the case may be. The PDPO empowers the Commissioner for the purposes of an inspection to enter premises and carry out investigations. The Commissioner also has the power, for the purposes of any investigation, carry out a hearing. Counsel and solicitors do not have right of audience, although they may appear if the Commissioner thinks fit.

Where the Commissioner has completed an inspection, he must inform the relevant data user of the result of the inspection and of any recommendations which he may make arising from the inspection. He may also publish a report setting out his recommendations in such manner as he thinks fit.

Where, following completion of an investigation, the Commissioner is of the opinion that the relevant data user is contravening a requirement under the PDPO, he may serve a written notice on the data user directing him to remedy and, if appropriate, prevent any recurrence of the contravention. An enforcement notice must:

- state that the Commissioner is of the opinion that there has been contravention of the PDPO by the data user;
- give his reasons for his opinion; and
- specify the requirement of the PDPO which in the opinion of the Commissioner is being contravened.

A data user who contravenes an enforcement notice commits an offence and is liable to a fine and to imprisonment for 2 years.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

(a) 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.

(b) DPP6 provides that 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

(a) Direct Marketing by data user

The PDPO requires that a data user intending to use direct marketing means (ie, by mail, fax, email or other means of communication, or by telephone calls to specific persons — and not at large) must:

(i) inform the data subject that:

- the data user has the intention of using his/her personal data for direct marketing;
- it may not use the personal data without his/her consent; and

(ii) provide him/her with details of:

- the kinds of personal data to be used in the direct marketing; and
- 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.

(iii) 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.

(b) Provision of personal data by the data user to a third party for direct marketing by that third party

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:

(i) inform the data subject in writing:

- of that intention; and
- that it may not provide the data without his/her written consent.

(ii) provide him/her with the following written information:

- confirmation that the data user is to provide the data for gain,
- the kinds of personal data to be provided,
- the classes of persons to which the personal data is to be provided, and
- the classes of marketing subjects in relation to which the personal data is to be used; and

(iii) provide the data subject with a channel through which the data subject may communicate his/her consent in writing without charge by the data user.

Unless the data user has complied with the above requirements and has received the written consent of the data subject either generally or selectively 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 who has been provided with information by a data user may, at any time, require the data user to cease to provide his/her 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.

The consent or the written consent of the data subject (as required by (a) or (b) above) may be given by way of:

- a general blanket consent by the data subject to the data user to the use of or the transfer of his/her personal data in respect of all kinds of personal data or all classes of marketing subjects as specified in the consent; or
- an express selection of a choice by the data subject to provide consent to some or all in the categories of:
  - the kinds of personal data held by the data user;
  - the classes of the full range of marketing subjects offered by the data user; and
  - 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is no regulation of tracking technologies from a privacy perspective.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertisement, being direct marketing, is governed by the PDPO (see question 8.1).

Under the PDPO a data subject may at any time require a data user to cease to use his/her 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 user 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 Unsolicited Electronic Messages Ordinance ("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 offer to supply goods, services, facilities, land or an interest in land;
- to offer to provide a business opportunity or an investment opportunity;
- to advertise or promote goods, services, facilities, land or an interest in land;
- to advertise or promote a business opportunity or an investment opportunity;
- to advertise or promote a supplier, or a prospective supplier, of goods, services facilities, land or an interest in land; or
- to advertise or promote a provider, or a prospective provider of a business opportunity or an investment opportunity, in the course of or in furtherance of business.

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;
- is sent to a telecommunications device in Hong Kong that is used to access the message; or
- is sent to 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 address oversea to Hong Kong 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 addressees, which may be given and withdrawn by means of an electronic message or in any other manner. It is safer to require and rely upon written consent or written withdrawal for the giving or withdrawal of such consent. If a person other than the registered user of an electronic address uses the relevant account to send an electronic message about consent or about the withdrawal of consent that person shall be treated as having been authorized to send that message on behalf of the registered user.

No person may acquire or supply or offer to supply the following to another person 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:

- address harvesting software,
- a right to use address harvesting software,
- a harvested address list, or
- a right to use a harvested address list.

Nor may a person use address harvesting software or a harvested address list in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses 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:

- 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
- 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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The PDPO provides that a data user proposing to carry out a matching procedure must make a request in the specified form to the Commissioner seeking his consent to the carrying out of that procedure.

"Matching Procedure" is defined as a procedure whereby personal data is collected for one or more purposes in respect of 10 or more data subjects and comparing it with personal data collected for any other purpose in respect of those data subjects where the comparison is either for the purpose of producing or verifying data or produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data may in either case be used whether immediately or at any subsequent time for the purpose of taking adverse action against any of those data subjects.

The Commissioner is required to determine a matching procedure request by taking into account the matters in Schedule 5 to the PDPO, which are, broadly, to check that the request is in line with the public interest, to ensure accuracy of any personal data produced or verified by the matching procedure and to identify the benefits to be derived from carrying out the matching procedure.

See question 8.1 as to the provisions of the PDPO controlling the intended transfer by a data user of the personal data of the data subject to a third party for direct marketing by that third party.

8.5 Are there specific privacy rules governing data brokers?

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 his/her personal data to a third party for use by that third person in direct marketing (as to which see question 8.1(b)).

8.6 How is social media regulated from a privacy perspective?

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, and of the UEMO relating to unsolicited electronic messages, all apply.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

There are no restrictions imposed by statute on data transfer. Section 33 of the PDPO, prohibiting 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

(a) As specified in question 6.2, a data user who contravenes an enforcement notice commits an offence and is liable to a fine and to imprisonment for two years.

(b) Offenses for non-compliance with the PDPO:

(i) Use by a data user of personal data in direct marketing and failing to give the relevant details to the data subject or provide a channel to indicate consent has a maximum penalty of a fine of $500,000 and imprisonment for 3 years;

(ii) Use by a data user of the personal data of a data subject in direct marketing without obtaining his/her consent to the intended use has a maximum penalty of a fine of $500,000 and 3 years imprisonment;

(iii) Use by a data user of the personal data of the data subject in direct marketing and failing to inform the data subject that the data user must, without charge, cease to use

the personal data in direct marketing if the data subject so requires has a maximum penalty of a fine of $500,000 and 3 years imprisonment;

(iv) Failure of a data user to comply with a request by a data subject to cease to use his/her personal data in direct marketing has a maximum penalty of a fine of $500,000 and 3 years imprisonment;

(v) Failure by a data user intending to provide personal data to another person for use in direct marketing to give the data subject all the required details in writing and to provide a channel by which to give consent has a maximum penalty (if for gain) of a fine of $1M and 5 years imprisonment, and a fine of $500,000 and 3 years imprisonment (if not for gain);

(vi) A data user providing the personal data of a data subject to another person for use in direct marketing by that other person without receiving the written consent of the data subject and, if for gain, having specified the intention to the data subject and ensuring that the provision of the data is consistent with the consent of the data subject, has a maximum penalty (if for gain) of a fine of $1M and 5 years imprisonment, and a fine of $500,000 and 3 years imprisonment (if not for gain);

(vii) Failure by a data user to comply with the request of a data subject to cease to provide his/her personal data for use in direct marketing or to notify any data transferee in writing to cease to use the data in direct marketing has a maximum penalty (if for gain) of a fine of $1M and 5 years imprisonment, and a fine of $500,000 and 3 years imprisonment (in any other case); and

(viii) Failure by a data transferee to comply with the written notification from a data user to cease using the personal data of a data subject in direct marketing has a maximum penalty of a fine of $500,000 and 3 years imprisonment.

(c) The following offences for knowing contravention of prohibitions in the UEMO carry a maximum penalty of a fine of $1M and 5 years imprisonment:

(i) Contravention of the prohibition on supply of address harvesting software or a harvested address list or the prohibition to use either;

(ii) Contravention of prohibition on acquisition of address harvesting software, harvested address list or the right to use either in connection with the sending of commercial electronic messages with a Hong Kong Link without the consent of the registered users of the electronic addresses to which they are sent;

(iii) Failure by a person to obtain the consent of the registered user of an electronic address to which are sent commercial electronic messages having a Hong Kong Link with the use of address harvesting software or a harvested address list; and

(iv) Contravention of the prohibition upon sending a commercial electronic message with Hong Kong Link to an electronic address obtained using an automated means.

10.2 Do individuals have a private right of action? What are the potential remedies?

As stated in question 10.1, the principal sanctions against breach of the statutory requirements of the PDPO or of the UEMO are criminal and attract fines and jail penalties.

Given that there is no law in Hong Kong expressly prohibiting freedom of expression, there are very few remedies at law that the data subject can turn to. There may be the possibility of an action for breach of confidence (see question 1.1).

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Hong Kong which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

No.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Hong Kong?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The 2013 amendments to the PDPO substantially extend the controls on direct marketing and are by far the strongest sanction on personal data privacy to date.

The introduction of these amendments was generated by a feeling that controls on direct marketing utilizing personal data were not adequate or sufficient and the stringent force of the amendments, with substantially increased penalties, was accordingly tabled and enacted in 2013.

12.2 What do you envision the privacy landscape will look like in 5 years?

The position is likely to remain stable in its present format.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Many provisions of the GDPR of the European Union 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 but there is no clear way forward yet in this in 2020.

INDIA

1 PRIVACY LAW

1.1 How is privacy regulated in India?

The right to privacy has been recognized as a fundamental right under Article 21 of the Constitution by the Supreme Court of India in the landmark judgment in the case of *Justice KS Puttaswamy (Retd) v Union of India* (August 2017).

Supreme Court of India in the case of *Rajagopal v State of Tamil Nadu* (1994) also elaborated on the scope of a privacy right and held that, unlike most fundamental right which apply only against the state (because of the state's ability to curb the freedoms of citizens), the right to privacy applies against both the state and fellow citizens, stating:

> "The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy."

In view of the above judgments of Supreme Court of India, the right to privacy is available to all citizens against any violation by governmental and private organizations.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Indian Contract Act 1872, Information Technology Act 2000 ("IT Act") and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("IT Rules") are the relevant statutes for protection of data or information:

(a) Indian Contract Act 1872 provides civil remedy in case of violation of contract in disclosing personal information without consent.

(b) The IT Act is the most important legislation which regulates the data privacy.

Section 43A of the IT Act (as amended in 2008) provides for compensation where a body corporate has failed to protect data due to its negligence in implementing and maintaining reasonable security practices and procedures which results in wrongful loss or wrongful gain to any person.

Explanation (ii) to Section 43A defines "reasonable security practices and procedures" as:

> "security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit".

(c) IT Rules: The above-mentioned provisions of the Information Technology Act 2000 are implemented in conjunction with the IT Rules, which have been framed to regulate the collection, processing/handling, disclosure etc of personal information by the organizations.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

No state or central authorities have been designated purely for the enforcement and regulation of data protection laws. However, any aggrieved person has the right to bring a matter of concern to a court of suitable jurisdiction. Where the claim for injury or damage does not exceed 50 million rupees, the Central Government appoints an adjudicating officer for holding an inquiry in the matter. The adjudicating officer has the powers of a civil court, and all proceedings before it are judicial proceedings.

2 SCOPE

2.1 Which companies are subject to privacy law in India?

All governmental and private organizations are subject to privacy laws.

2.2 Does privacy law in India apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Section 75 of the IT Act specifies that the provisions of this Act apply to any offence or contravention committed outside India by any person (including companies), irrespective of his nationality. The provisions of the IT Act apply only if the act/conduct constituting the offence/contravention involves a computer, computer system or computer network located in India.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in India?

"Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive personal data or information" of a person means such personal information which consists of information relating to password; financial information, such as bank account or credit/debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information.

However, any information that is freely available or accessible in public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force will not be regarded as sensitive personal data or information.

The specific obligations in relation to sensitive information are as follows:

(a) Consent has to be obtained in writing by letter, fax or email from the provider of the sensitive personal data or information regarding the purpose of use before collection of such information.

(b) Sensitive personal data or information may not be collected unless:

(i) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(ii) the collection of the sensitive personal data or information is considered necessary for that purpose.

(c) A body corporate or any person on its behalf holding sensitive personal data or information may not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(d) Disclosure of sensitive personal data or information by a body corporate to any third party requires prior permission from the provider of such information, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation.

(e) A body corporate or any person on its behalf may not publish sensitive personal data or information.

(f) A third party receiving sensitive personal data or information from a body corporate or any person on its behalf may not disclose it further.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

(a) The body corporate or any person who on its behalf, collects, receives, possess, stores, deals or handle personal information must provide a privacy policy for handling of or dealing in personal information. Such policy shall be published on its website and must provide:

(i) clear and easily accessible statements of its practices and policies;

(ii) the type of personal or sensitive personal data or information collected; and

(iii) the purpose of collection and usage of such information.

(b) The body corporate or any person on its behalf must, prior to the collection of information including sensitive personal data or information, give the provider of the information the option not to provide the data or information sought to be collected.

(c) The provider of information must also have the option to withdraw its consent, at any time, while availing the services or otherwise.

(d) A body corporate or any person on its behalf may transfer sensitive personal data or information to any other body corporate or person in India, or located in any other country that ensures the same level of data protection that is adhered to by the body corporate. Such transfer is allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and the provider of the information, or where such person has consented to data transfer.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The current IT Act and IT Rules do not recognize the term "data processor". However, the Personal Data Protection Bill 2018, which has not yet been brought into force, defines "data processor" as "any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary".

The Bill further provides that the data fiduciary may only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract. The data processor must not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorisation of the data fiduciary, unless the contract so permits. The data processor, and any employee of the data fiduciary or the data processor, may only process personal data in accordance with the instructions of the data fiduciary, unless they are required to do otherwise by law, and must treat any personal data that comes within their knowledge as confidential.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

This question has been covered in previous sections.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in India? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

A body corporate/person on its behalf will be considered to have complied with reasonable security practices and procedures if it has implemented such security practices and standards, and has a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures, that are commensurate with the information assets being protected and with the nature of business. The international Standard IS/ISO/IEC 27001 on "Information Technology — Security Techniques — Information Security Management System — Requirements" is one such standard.

Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection, must get its codes of best practices duly approved and notified by the Central Government for effective implementation. The body corporate/person on its behalf which has implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified by the Central government, will be deemed to have complied with reasonable security practices and procedures, provided that such standard or the codes of best practices have been certified or audited

on a regular basis by an independent auditor, duly approved by the Central Government. Such audit of reasonable security practices and procedures should be carried out by an auditor at least once a year, or as and when the body corporate/person on its behalf undertakes a significant upgrade of its process and computer resource.

6.2 How are data breaches regulated in India? What are the requirements for responding to data breaches?

In the event of a data security breach, the body corporate or a person on its behalf will be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Right to privacy has been recognized as a fundamental right under Article 21 of the Constitution by the Supreme Court of India. Therefore, right to privacy is available to all citizens against any violation by governmental and private organizations.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

There are no statutory regulations governing marketing communication through emails.

Advertising through unsolicited calls and messages is regulated by the Telecom Regulatory Authority of India ("TRAI"). TRAI has issued the Telecom Commercial Communication Customer Preference Regulations 2010 to curb a growing menace, and effectively regulate unsolicited commercial calls and messages. TRAI has also issued a notification prohibiting unsolicited commercial communications ("UCC") through SMS. All mobile operators have to prefix an identification tag before all application-to-peer ("A2P") SMS texts sent from their SMS centers.

TRAI has used multiple means to deter SMS spam and unsolicited telemarketing, including mandatory registration for telemarketing and SMS marketing, which includes provisions requiring marketers to respect a nationwide "Do Not Call" list, the Telecom Commercial Communications Customer Preference Portal ("NCCP"). TRAI additionally approaches this from a pricing perspective, levying higher termination charges for transactional SMS texts to raise the costs of bulk SMS and make it uneconomical to send unsolicited SMS campaigns.

The NCCP is a database containing a variety of information prescribed in the Telecom Commercial Communications Customer Preference Regulations 2010.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The current IT Act and IT Rules do not address issues relating to use of tracking technologies (eg, cookies, pixels, SDKs).

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The current IT Act and IT Rules do not address issues relating to targeted advertising and behavioral advertising.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The current IT Act and IT Rules do not specify the type of notice and consent required.

8.5 Are there specific privacy rules governing data brokers?

There are no specific privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

The statutes and regulations discussed above also apply to social media. There are no specific regulations concerning social media from privacy perspective.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

The statutes and regulations discussed above also apply to loyalty programs and promotions. There are no specific regulations concerning loyalty programs and promotions.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

A body corporate or any person on its behalf may transfer sensitive personal data or information to any other body corporate or a person in India, or located in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer will be allowed only if it is necessary for the performance of the lawful contract between the body corporate/any person on its behalf and the provider of information, or where such person has consented to data transfer.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

No.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate will be liable to pay damages by way of compensation to the person so affected.

10.2 Do individuals have a private right of action? What are the potential remedies?

The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. Therefore, individuals have a private right of action. Potential remedies include damages by way of compensation. Further, the IT Act specifies that if any person, including an intermediary, who, while providing services, has secured access to any material containing personal information about another person with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, he will be punished with imprisonment for a term of up to three years, or with a fine of up to 500,000 rupees, or with both.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of India which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The Personal Data Protection Bill 2018 for regulating the processing of personal data of individuals (data principals) by government and private entities (data fiduciaries) incorporated in India and abroad, has been introduced by the government of India. This Bill, when enacted, will bring about a dramatic change in the privacy laws.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in India?

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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

The Supreme Court of India, in *Justice KS Puttaswamy (Retd) v Union of India,* has recently recognized the right to privacy as a fundamental right, emerging primarily from Article 21 of the Constitution. With the recognition of privacy as fundamental right, a need has arisen for a comprehensive data protection framework to unlock the data economy while keeping the data of citizens secure and

protected. This has led to the introduction of the Personal Data Protection Bill 2018, which is yet to be brought into force.

12.2 What do you envision the privacy landscape will look like in 5 years?

The enactment of the Personal Data Protection Bill 2018 will enhance data protection and minimise intrusion into the privacy of an individual caused by the collection and usage of their personal data.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The changing privacy landscape creates significant risks for the companies. Changing regulatory requirements is one of the main concerns of the companies. Also, data privacy challenges and risk of litigation is ever increasing.

ISRAEL

1 PRIVACY LAW

1.1 How is privacy 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 by the Constitution, Law and Justice Committee of the Knesset, to set regulations and issue orders.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Though Israel does not have a written constitution, there are a set of "Basic Laws" which have a constitutional status. According to Section 7 (Human Dignity and Liberty) of the Basic Law, all persons have a right to privacy and intimacy.

The PPL is the primary law relating to privacy. It generally governs two types of "privacy". The first deals with the "classic" privacy rights to which individuals are entitled. The second relates to databases, namely, collecting, storing and handling information/data.

The Minister of Justice, in accordance with his powers pursuant to the PPL, has set a number of regulations and orders, including, but not limited to:

(a) The Privacy Protection Regulations (Information Security) 2017;

(b) The Privacy Protection Regulations (Transferring Information to Databases Outside Israel) 2001;

(c) The Privacy Protection Regulations (Setting Databases which Include Information not to be Exposed) 1987;

(d) The Privacy Protection Regulations (Conditions for Holding and Securing Information and Methods of Transferring Information between Public Bodies) 1986; and

(e) The Privacy Protection Regulations (Conditions for Reviewing Information and Legal Procedure of Appealing a Refusal to Reveal Information) 1981.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

First and foremost, privacy law is enforced by the Israeli courts. If an individual considers that his privacy has been infringed, he may bring a civil action against the infringer before a court of law.

Extreme intentional 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, 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 SCOPE

2.1 Which companies are subject to privacy law in Israel?

The PPL and the regulations derived from it, apply to individuals and all types of companies. Moreover, the PPL applies to State of Israel and public bodies, such as governmental offices, cities, municipalities and all bodies which fulfil public roles.

2.2 Does privacy law in Israel apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The PPL can be divided into two parts. 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 may not infringe the privacy rights of Israelis.

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 and its derived regulations relate 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 INFORMATION

3.1 How is personal information/personal data defined in Israel?

Under Section 7 of 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

(a) Under Section 7 of the PPL, "sensitive information" means:

  (i) data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; and

  (ii) 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.

(b) According to the Consumer Protection Regulations (Advertisements and Marketing Methods Targeted at Minors) 1991, it is prohibited to use information relating to minors for advertising and marketing purposes, without parental or guardian consent.

(c) According to court rulings, an individual's credit card information is considered sensitive information.

(d) Information relating to state security is considered sensitive, as is biometric data.

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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Companies, *inter alia*, need to define within a "definition document", the methods of gathering and the use of the data, the objects of the data's use, the risks, the appointment of a database manager and supervisor. The Information Security Supervisor (see question 2.4) must set security procedures, and ensure that only authorized individuals have access to the stored information.

The Privacy Protection Regulations (Information Security) 2017 defines four types of databases:

(a) Databases bound by the strictest security obligations;

(b) Databases with medium security obligations;

(c) Databases with basic security obligations; and

(d) Databases managed by an individual which are bound by relatively lenient obligations.

It should be noted that certain types of databases require registration at the Database Registry. According to the PPL, a database owner, including a company, is obligated to register his database if one of the following applies:

(1) the database contains information on more than 10,000 persons;

(2) the database contains sensitive information;

(3) the database includes information on persons, and the information was not delivered to this database by them, on their behalf, or with their consent;

(4) the database belongs to a public body; or

(5) the database is used for direct-mailing services.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

First and foremost, under the PPL, the owner of a database is responsible for securing stored information/data. Under the Privacy Protection Regulations (Information Security) 2017, companies/individuals, excluding sole individuals managing data bases or sole owned companies, must appoint an Information Security Supervisor.

The Privacy Protection Regulations (Information Security) 2017 define "Information Security Supervisor" and "Database Manager". The Database Manager is responsible for the Information Security Supervisor, who must report to the Manager.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

First and foremost, under the PPL and its derived regulations, it is prohibited to infringe an individual's privacy, unless the individual provides his consent. Namely, one may not use for profit a person's image, voice, name and personal affairs. Hence, advertisers should obtain clear consent from the subject appearing in their advertisements. When minors appear in advertisements, parental or guardian consent must be provided.

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.

As mentioned in question 2.3 above, if the stored data falls under certain criteria, the database owners, are required to register their database with the Database Registrar.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Israel? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is regulated by the PPL and the Privacy Protection Regulations (Data Security) 2017. There are different types of data bases, namely:

(a) Databases held by an individual;

(b) Databases which are subject to a basic level of security;

(c) Databases which are subject to a medium level of security;

(d) Databases which are subject to high level of security; and

(e) Biometric databases.

The Privacy Protection Regulations (Data Security) 2017, clearly prescribe the method of classifying different types of databases. Once a database holder identifies the type of database he owns, he may observe the applicable rules.

6.2 How are data breaches regulated in Israel? What are the requirements for responding to data breaches?

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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

First and foremost, Israelis have a constitutional right to privacy under the Basic Law: Human Dignity and Liberty. Under the PPL, individuals have a right not to have their privacy infringed.

Individuals have a right to inspect their personal information which is stored in databases. Further, individuals have the right to request that the information relating to them is accurate and complete.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications are regulated by the Israel Communications Act (Telecommunications and Broadcasting) 1982. Under the Israel Communications Act (Telecommunications and Broadcasting) 1982, it is prohibited to market via emails, texts, push notifications or automatic dialling without receiving unequivocal consent from the addressee prior to sending the communication. Accordingly, Israel is considered an "opt in" country.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Cookies, in their traditional meaning (ie, assisting a website user by negating the need to re-register his particulars) seem legal. However, the use of a person's registered information by third parties for marketing purposes is problematic, to say the least.

The PPL and the Israel Computers Law 1995 regulate the above topics.

According to Section 2(9) of the PPL, "using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given" is considered an infringement of privacy.

According to Section 4 of the Israel Computers Law, a person who unlawfully "penetrates computer material" located in a computer is liable to imprisonment for a period of three years; "penetration into computer material" means penetration by means of communication or connection with a computer, or by operating it, but excluding penetration into computer material which constitutes eavesdropping under the Eavesdropping Law 1979.

Clearly, the law in Israel relating to cookies is outdated. However, it seems that if:

(a) an individual gives his consent to the use of cookies, and

(b) the user discloses the purposes of the cookies and the fact that information will be transferred to third parties,

then the use of cookies will be legal.

8.3 How is targeted advertising and behavioural advertising regulated from a privacy perspective?

Under Section 2(9) of the PPL and Section 4 of the Computers Law (see question 6.2), it would seem the legality of behavioural advertising should be determined by knowledge and consent. Hence, if the consumer knows beforehand who is going to use the information he provides and for what purposes, behavioral advertising should be legal.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

When targeting consumers by means of information obtained from customer matching databases, the advertiser/marketer must give the following information to the consumer:

(a) that the information has been obtained from a consumer matching database, and identify the database,

(b) the consumer's right to be deleted from the database and

(c) the precise identity of the database owner.

8.5 Are there specific privacy rules governing data brokers?

First and foremost, as prescribed in the PPL, data brokers need to register their database at the Database Registry. Within the registration, the broker must disclose:

(a) the identity of the database registrant;

(b) the purpose of the database;

(c) the type of stored data;

(d) the source of the collected data; and

(e) the methods of obtaining the data.

8.6 How is social media regulated from a privacy perspective?

The topic of social media is not regulated by separate and specific laws. The general provisions described above apply to social media. Thus, it is prohibited to infringe a person's privacy by any means or methods, including social media.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The transfer of data is regulated in the Protection of Privacy Regulations (Transfer of Data to Data Bases Outside State Borders) 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 lesser than the level of protection of data provided for by Israeli Law, and the following principles shall 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;

(e) The obligation to take adequate security measures to protect data in databases is mandatory.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

An Israeli company may transfer data to a company outside Israel if the receiving company is controlled by the transferring company, and the receiving company ensures privacy protection.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 between NIS 50,000–100,000 (approximately US $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.

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 various orders, including publishing its rulings and destroying material which violates privacy.

10.2 Do individuals have a private right of action? What are the potential remedies?

As described above in question 8.1, individuals have a right of action resulting in the remedies described above.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Israel which affect privacy?

N/A

11.2 Are there any hot topics or laws on the horizon that companies need to know?

N/A

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Israel?

N/A

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Following unfortunate incidences in which nursery school children were harmed by staff, a public outcry resulted in the enactment of the Instalment of Cameras for the Protection of Toddlers in Daycare Nurseries 2018. Unfortunately, senior citizens have also been victims of mistreatment by staff in retirement homes as have the mentally challenged in care facilities.

In short, weaker individuals are often harmed by those who are entrusted with their protection and care. Thus, similarly to daycare nurseries, it is quite possible that in the future, cameras will be installed in retirement homes, hospitals and other facilities for the weak and helpless.

Further, there is presently wide use of cameras in municipalities and cities which monitor inhabitants in public places. The use of cameras will definitely increase in the future. Hence, in addition to monitoring individuals in the web, we can expect increased monitoring of our activities on camera.

12.2 What do you envision the privacy landscape will look like in 5 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 relatively respects privacy rights, it is not at par with the European Union. One can expect changes in the local legislation which mimic the GDPR**.**

Additionally, at present, the law in relation to foreign companies, especially in the areas of storing, handling and transferring data, is unclear. Hence, more thought and regulation will be needed to address Israeli privacy legislation *vis à vis* foreign companies.

12.3 What are some of the 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.

JAMAICA

1 PRIVACY LAW

1.1 How is privacy regulated in Jamaica?

Privacy is minimally regulated in Jamaica.

Currently, the right to privacy is expressly contained in Jamaica's Constitution pursuant to the Charter of Fundamental Rights and Freedoms in Chapter Three.

The right to privacy is also referred to in the Copyright Act of 1993 (last amended 2015) in relation to photographs and films.

The Government has an ICT Policy (March 2011) which addresses the issue of digital privacy of customer information. This states:

> "Privacy of customer information can be compromised by virtue of unauthorized access. It is, however, recognized that in certain specific circumstances (national security and defence) provision may be made for access to personal information. Possible violations include archiving of personally identifiable customer information for marketing and sales purposes without prior written or electronic consent, and failure to disclose policy regarding usage of information, unauthorized recording of communication and installation of rogue programmes."

The objective is to minimize the risks of the unauthorized access and the disclosure of customer information. Against this background, the government has committed to passing legislation which, among other things, will impose sanctions for the invasion of privacy, unauthorized access and unauthorized use of customer information.

A Data Protection Bill is currently before the Joint Select Committee of Parliament. The public was invited to submit comments on the Bill, and the Joint Select Committee will then make recommendations for changes to the Bill before it is passed. The government anticipates that the Bill will be passed by March 2020.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Please see above.

The Charter of Fundamental Rights and Freedoms in Chapter Three of the Jamaican Constitution provides for:

> "The right to 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."

The Copyright Act recognizes the right to privacy in photographs and films. A person who commissions the taking of a photograph or the making of a film for domestic or private purposes can prevent the copying, broadcasting and other commercial use of such photograph or film.

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.

There are other statutes in Jamaica which impact on privacy, including:

(a) Interception of Communications Act 2002;

(b) Cyber Crimes Act 2015;

(c) Access to Information Act 2002; and

(d) the old Official Secrets Act.

The Interception of Communication Act makes it unlawful for a person to intentionally intercept communications transmitted by means of a telecommunications network.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

There are currently no regulatory bodies which specifically enforce privacy laws.

The draft Data Protection Bill provides for the creation of an office, to be known as the Information Commissioner, to monitor and enforce compliance with the data protection laws.

2 SCOPE

2.1 Which companies are subject to privacy law in Jamaica?

All companies operating in Jamaica are subject to the laws of Jamaica.

2.2 Does privacy law in Jamaica apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

N/A

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Jamaica?

"Personal data" is defined in the draft Data Protection Bill as:

> "data relating to a living individual who can be identified:
>
> (a) from the data; or
>
> (b) from the data and other information in the possession of, or likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The draft Data Protection Bill defines "sensitive personal data" as consisting of any of the following information in respect of a data subject:

(a) genetic data or biometric;

(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 commission or alleged commission of any offence by the data subject or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The draft Data Protection Bill provides eight standards for the processing of data:

(a) First Standard: Personal data shall be processed fairly and lawfully.

(b) Second Standard: Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes.

(c) Third Standard: Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processes.

(d) Fourth Standard: Personal data shall be accurate and where necessary, kept up to date.

(e) Fifth Standard: Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

(f) Sixth Standard: Personal data shall be processed in accordance with the rights of data subjects.

(g) Seventh Standard: Appropriate technical and organizational measures shall be taken:

  (i) against unauthorised or unlawful processing of personal data and against accidental loss or destructions of, or damage to personal data;

  (ii) to ensure that the Commissioner is notified, without any undue delay, of any breach of the data controller's security measures which affect or may affect any personal data.

(h) Eighth Standard: 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 (see also questions 9.1 and 9.2).

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

"Data controller" is defined in the draft Data Protection Bill 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 who the obligation to process the data is imposed by or under that enactment is for the purposes of this Act a data controller".

On the other hand, 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".

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The draft Data Protection Bill provides several obligations on the part of the data controller:

(a) Registration: The Information Commissioner must maintain a register of all data controllers. Personal data must not be processed by any data controller unless the registration particulars of that data controller are included in the register. Failing to do so is an offence under the Bill.

(b) Appointing a data protection officer: 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.

(c) Data impact assessments: A data controller must submit a data impact assessment in respect of all data in its custody or control within 90 days of the end of the calendar year.

The Information Commissioner may request an impact assessment on behalf of an individual who is directly affected by processing of personal data by that data controller.

The Information Commissioner may also issue assessment notices or information notices to determine whether a data controller is acting in compliance with the law.

(d) Duty to comply with data protection standards: It is the duty of a data controller to comply with the data protection standards in relation to all personal data with respect to which it is the data controller.

Even companies located outside of EU jurisdiction must comply with the General Data Protection Regulation ("GDPR") if they process the personal data of EU citizens, who are the primary beneficiaries of the law.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Jamaica? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

N/A

6.2 How are data breaches regulated in Jamaica? What are the requirements for responding to data breaches?

Under the draft Data Protection Bill, 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The Charter of Fundamental Rights and Freedoms provides for the right of everyone to:

(a) protection from search of the person and property;

(b) respect for and protection of private and family life, and privacy of the home; and

(c) protection of privacy of other property and of communication;

Under the draft Data Protection Bill, a data subject will also have the following rights:

(d) right of access to personal data;

(e) right to prevent processing likely to cause damage or distress;

(f) right to prevent processing for purposes of direct marketing;

(g) rights in relation to automated decision-taking; and

(h) right to rectification of inaccuracies.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

There are currently no regulations for marketing communications from a privacy perspective.

Under the draft Data Protection Bill, an individual is entitled at any time, by notice given orally or in writing to a data controller, to require the data controller not to, or to cease processing that individual's personal data for the purposes of direct marketing.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There are currently no regulations on tracking technologies.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There are currently no privacy regulations for targeted advertising and behavioural advertising.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

There are currently no regulations for notice or consent for advertisers to share data with third parties for customer matching.

8.5 Are there specific privacy rules governing data brokers?

No. There are no specific privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

There are currently no privacy regulations for social media.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There is currently no regulation of loyalty programs from a privacy perspective.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Under the draft Data Protection Bill, the eighth standard for the processing of personal data 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 subjections.

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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Under the draft Data Protection Bill, the eighth standard (see question 9.1) 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 subjection.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Penalties and sanctions under the incoming Data Protection Act are expected to be included in Data Protection Regulations, which have not yet been drafted.

There are also remedies under the Law of Confidence for breach of confidence.

10.2 Do individuals have a private right of action? What are the potential remedies?

No. Individuals do not have a private right of action. However, if information is disclosed in confidence, there is a right of action for breach of confidence.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Jamaica which affect privacy?

While there are no rules particular to Jamaica which affect privacy, the incoming Data Protection Act will certainly have a major impact on the culture of doing business in Jamaica.

This will be a major change for Jamaican companies, as there are currently no real restrictions on the processing and use of an individual's data, and data is often shared with other companies for the purposes of marketing.

Due to the implementation of the European Union's GDPR, and the pending Data Protection Act, companies in Jamaica are being sensitized to the GDPR, and some companies that handle information of EU citizens are taking steps to implement its regulations.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The draft Data Protection Act and accompanying Data Protection Regulations will have a major impact on companies once enacted. The Cyber Crimes Act is also due for review. There is also a National Identification Bill which has privacy implications. In its original format, it was deemed unconstitutional in relation to the Constitutional right to privacy. It has been subsequently amended to remove the infringing portions of the Bill.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Jamaica?

Although the Data Protection Act has not yet been enacted, 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 even before the Act comes in to force.

Companies in Jamaica are advised to start preparing to meet the data protection standards. Whilst the Bill is still being reviewed and some changes will be made, it is not likely that the data protection standards will be altered, as they are based on the EU's data protection standards.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

As indicated in the draft Data Protection Bill's Memorandum of Objects and Reasons, Jamaica's treaty obligations (CARIFORUM) under the Economic Partnership Agreement entered into with the European Union require it 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 do you envision the privacy landscape will look like in 5 years?

With the enactment of the Data Protection Act, we anticipate that the privacy landscape will be far more developed. It is expected that companies will be given a transition period to ensure compliance once the Act comes into effect.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The Data Protection Act, when passed, will be transformative to Jamaica, as there will have to be major adjustments in current practices for companies to ensure compliance.

JAPAN

1 PRIVACY LAW

1.1 How is privacy 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) **Privacy generally:** 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.

(b) **Personal Information:** Personal information is primarily protected under the Act on Protection of Personal Information ("APPI") and related guidelines which govern the collection, storage, usage and processing of personal information in Japan. The Act on the Protection of Personal Information Held by Administrative Organs and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc protect personal information in the public sector.

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.

General Guidelines relating to the APPI (which are applicable to all private sectors) cover matters such as transfers of personal information to a third party in a foreign country, obligations due diligence and recordkeeping when transferring personal information to a third party, and data anonymization.

Certain ministries have been delegated authority to issue guidelines for the implementation of the APPI for the industries they regulate (the "Sector-Specific Guidelines"). There are Sector-Specific Guidelines in the finance, healthcare, telecommunication and postal sectors (issued by 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).

There are also supplementary rules on the handling of personal data transferred from the European Union on the basis of the EU adequacy decision concerning the APPI.

(c) **Self-regulation — Privacy Mark System:** 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 (JIS Q 15001 Personal Information Protection Management System — Requirements) 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.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The right to privacy and personal information protection law is enforced through the courts, bar associations, the Personal Information Protection Committee ("PPC") and other regulators in certain business sectors.

A person who believes their privacy rights have been infringed can apply to a court for injunctive relief and/or compensation for damages suffered.

The Japan Federal Bar Association ("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"):

(a) accepts requests for human rights relief from victims of human rights violations and related persons, including a person who is violated regarding his/her privacy,

(b) investigates the facts of the requests and the facts of the violations, and

(c) when it finds that human rights violations or human rights violations are likely to occur, aims to eliminate or improve human rights violations by taking measures such as:

  (i) warnings (providing its opinions and urging an appropriate response),

  (ii) recommendations (providing its opinions and seeking appropriate responses), or

  (iii) requests (providing its opinions and requesting appropriate response) against human rights offenders or their supervisory authorities.

In order to ensure that the measures taken 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.

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 SCOPE

2.1 Which companies are 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) colleges, universities, other institutions or organizations engaged in academic studies, or entities belonging to them for the purpose of academic studies;

(d) religious organizations for the purpose of religious activities (including incidental activities); and

(e) political organizations for the purpose of political activities (including incidental activities).

However, each entity handling personal information listed above 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.

The exemption from the APPI for business operators handling small amounts of personal information was abolished in 2017.

"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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 the said 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 accurate and up-to-date, and to delete it when no longer required;

(c) to take measures to protect the data against leaks, etc.;

(d) to supervise employees handling personal information 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 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.

Although the PPC cannot enforce its orders for compliance with the APPI, etc, against such an offshore PIC, it may provide information to foreign regulatory authorities for their own regulatory enforcement purposes.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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) those 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 (meaning an electronic, magnetic or other forms 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) those 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 ID number;

(iii) unique characters, numbers, symbols and other codes designated by the Enforcement Ordinance 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"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 the consent from the data subject in order to obtain or transfer sensitive personal information unless one of the exceptions discussed at question 9.1(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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The key obligations of a PIC are set out at question 3.2; there are no specific obligations under Japan's privacy laws.

Neither privacy law nor data protection law imposes specific obligations on advertising. As general matters under the APPI, companies have to post their privacy policy and handle privacy and personal information in accordance with the privacy policy.

A PIC is not required to appoint a data protection officer, though the PPC suggests that a PIC appoint a person responsible for handling personal information. Certain private organizations or associations have created qualifications as "data protection officer" or equivalent, and issue them to persons who have passed examinations set by them.

A PIC is required to keep records of the transfer of personal information (see question 3.3 above) and should supervise any data processor appointed by it and take appropriate measures to secure personal information held by it.

A PIC is not required to register with the PPC or any other body.

If a PIC wishes to use an opt-out to effect a transfer of personal information without the consent of the data subject, it must first file the opt-out with the PPC.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Japan? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The APPI requires a PIC to take necessary and appropriate action for the security control of personal data held by it, including preventing the leak, loss or damage of the handled 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.

6.2 How are data breaches regulated in Japan? What are the requirements for responding to data breaches?

The PPC has issued guidelines in relation to requirements for responding to data breaches, which state that it is desirable to take the following actions following a data breach:

(a) internal reporting and prevention of expansion or aggravation of any damage;

(b) investigation of the facts and investigation of the cause;

(c) identification of the scope of the impact of the breach;

(d) review and implementation of measures to prevent a recurrence;

(e) prompt contact with the affected person(s) unless the leaked data is encrypted at a high level; and

(f) publication of facts and measures to prevent a recurrence.

The PIC must also make efforts to promptly notify the PPC of a breach unless:

(a) the leaked data is encrypted at a high level;

(b) all the leaked data has been collected by the PIC prior to being seen by third parties;

(c) there is no risk of any specific individual being identified from, or the affected data subjects being harmed by use of, the leaked data;

(d) the data loss was obviously only internal and not an external leak; or

(e) the leak is obviously insignificant (eg, a misdelivery 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. This is particularly so as "desirable", "make efforts" and "promptly" are not defined in the data breach guidelines.

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.

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, 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 issues guidance on what actions the PIC should take.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

If requested by a data subject, a PIC must disclose, in writing and without delay, to the data subject the data subject's personal data held by it, unless the data subject has agreed to receiving it by other means (eg, as electronic data). Access can be refused if it would result in:

(a) injury to the life or bodily safety, property or other rights and interest of the data subject or any third party;

(b) a material interference with the PIC's business operations; or

(c) a violation of other Japanese laws prohibiting disclosure.

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 if this is used for a purpose other than the one originally stated, or if it was acquired by fraudulent or other unlawful means. 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).

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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 expressly indicating 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 or specified rights (such as (i) the right to use a facility or to receive a service, which is sold in a transaction connected with people's daily lives, (ii) a corporate bond or other monetary claim; and (iii) a share in a stock company or a partnership interest, etc) it is prohibited, under the Act on Specified Commercial Transactions ("ASCT"), for a seller or a service provider to advertise via email, etc (ie, by sending advertising texts or any other data by electronic or magnetic means in a way that causes it to be displayed on the screen of the computer used by the advertising target) with regard to the terms and conditions under which the seller or the service provider sells goods or specified rights or provides services through mail order sales, 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 that has obtained an advertising target's consent or request to send a mail order email 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

In Japan, the use of tracking technologies such as cookies by companies is not regulated, though some companies have voluntarily adopted a "Cookie Policy".

However, the PPC is considering regulating the use of cookies by companies after it was detected that cookies and other information were used to identify individuals on a job-hunting information site for students. The Fair Trade Commission has also taken issue with the monopolization of the market by platforms and has begun to consider restricting the use of cookies.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There are no specific regulations on targeted advertising and behavioral advertising.

However, the Japan Interactive Advertising Association ("JIAA"), constructed by companies involved in the internet advertising business such as media and advertising companies, has produced Guidelines on Targeting Advertising.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

If the data falls within the scope of personal information under the APPI, the transfer consent requirements and restrictions under the APPI would apply (see question 3.3 above).

8.5 Are there specific privacy rules governing data brokers?

No, 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 General Guidelines (see question 9.1(c) below).

8.6 How is social media regulated from a privacy perspective?

There is no specific regulation on social media from a privacy or data protection perspective.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There is no specific regulation on loyalty programs and promotions from a privacy or data protection perspective.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

(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 9.2 below) (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 are 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 transfer of the 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:

(1) this joint use,

(2) the items of the personal data used jointly,

(3) the extent of the joint users,

(4) the purposes of joint use, and

(5) 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.

Where a transfer of personal data is to a person or entity which is not a third party, further transfer of the personal data by that person or entity would be subject to the consent rules and exceptions applicable to such transfers described in this article.

(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:

(1) 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; or

(2) implements data protection standards equivalent to those which PICs subject to the APPI must follow.

As of the date of this article only countries in the European Union and the European Economic Area are on the list of countries. If the country of the transferee is not in the EU/EEA, a transferor PIC would have to rely on the transferee implementing data protection standards equivalent to the APPI in order to effect a transfer of personal information offshore without the data subject's consent or in reliance on an exception listed above. Such an equivalent standard can be satisfied by the transferor and the transferee (a) entering into a contract; or (b) if they are in the same corporate group, 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 (c) 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).

On July 17, 2018, the European Union and Japan agreed to recognize each other's data protection regimes as providing adequate provisions for the protection of personal information (see question 12.1(c) below).

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

(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 9.1(a)) or the transferee is not a third party.

Thus, the transferor must keep a record of:

(i) (if the transfer was made in reliance on an opt-out) the transfer date;

(ii) the name or other identifier of the transferee and the data subject, and the type(s) of data transferred (eg, name, age, gender); and

(iii) 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.

The transferee must keep a record of:

(iv) (if the transfer was made in reliance on an opt-out) the date it received the personal data;

(v) 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;

(vi) the type(s) of data transferred;

(vii) 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;

(viii) if an opt-out has been relied on, the fact that the opt-out has been filed with, and published by, the PPC; and

(ix) 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 utilisation;

(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.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 their 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.

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, to possible criminal imprisonment for up to 6 months or a criminal fine of up to JPY 300,000, and the same criminal fine for the PIC as an entity.

In addition, 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 individuals have a private right of action? What are the potential remedies?

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 are rare.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Japan which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

It is expected that APPI will be revised in 2020, and companies need to be aware of the amendments. (Please see question 12.1 below.)

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Japan?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Japan's data protection laws had not been updated for many years and were seen to be falling behind the regimes in other developed countries, notably those of the European Union, and there was a public perception that personal information may be misused. As a result, the APPI was substantially revised in 2017, and a new oversight regime based on the PPC (which was established on January 1, 2016) introduced. The primary revisions are:

(a) Traceability requirement: a new regime to require due diligence and record-keeping on data transfers (see question 9.2 above);

(b) Use of encrypted anonymous data: through clarification of the definition of "personal information" and defining "encrypted anonymous information", use of such encrypted anonymous information will be liberalized and accelerate the use of big data;

(c) Transferring personal data overseas: the PPC held discussions with the European Commission in order to establish a framework on the APPI to ensure the smooth and mutual transfer of personal data between Japan and the European Union. With the coming into force of the General Data Protection Regulation ("GDPR"), the PPC obtained a decision of an "adequate level" of protection from the European Commission. This has resulted in a new

regime of frictionless transfers of personal information between Japan and the European Union coming into effect on January 23, 2019, creating what the EU Commission described as "the world's largest area of safe transfers of data based on a high level of protection for personal data". The PPC has issued supplementary rules to the APPI to give effect to the adequacy decision;

(d) Abolition of the exemption from the APPI of holders of small amounts of personal information; and

(e) Requirements governing the use of "opt out(s)" for consent to data transfers (see question 9.2(b)).

12.2 What do you envision the privacy landscape will look like in 5 years?

(a) Privacy protection will be strengthened with a view to protecting privacy not only in Japan but also in other countries, such as the European Union Member States, around the world.

(b) On the other hand, since the demand for the use of big data and other data is increasing, it is expected that new rules will be established to enable the use of data widely, after making the data pseudonymized and anonymized.

(c) The PPC is considering revising the APPI, according to the "Summary of Outline" as follows:

(i) Data subjects' rights

- Expand data subject's rights by relaxing the requirements for the entitlement for requiring data controllers to cease using or transferring personal data;
- Abolish the exemption for personal data held by a data controller only for six months or less from data subject's rights to access, etc; and
- Tighten the scope of the "Opt-out" exception to the general requirement for data subject's consent to data transfers.

(ii) Obligations of a data controller

- Make data breach notifications to the PPC and affected data subjects "obligations" of the data controller if certain criteria (ie, number of affected data subjects, etc) is met (under the current rules, the data controller is only "required to make efforts" to notify to the PPC and it is only "desirable" to notify the affected data subjects);
- Not change the timing required for the first breach notification to the PPC from the current requirement "sumiyakani" (meaning promptly, not specifying a specific deadline), but allow the PPC to set a specific deadline date for updated/conclusive investigation reports/recurrence prevention measure reports; and
- Clarify that a data controller must not use personal information "in an inappropriate manner".

(iii) Measures to promote better protections by data controllers

- Expand the scope of matters which a data controller is required to publish (eg, protection measures, details of how it processes personal data).

(iv) Data utilization

- Introduce rules for "pseudonymized" data (between personal data and anonymized data). Whilst controllers' obligations in handling pseudonymized data will be relaxed, transfers of such data to third parties will be restricted;
- Apply regulations on personal data transfers where the subject data is not personal data for a transferor, but it is for a data transferee; and
- Add more examples of data transfers allowed without consent due to public interest.

(v) Penalties

- Review the criminal penalties under the current APPI.

(vi) Expand the scope of extra-territorial application of the APPI

- Make offshore controllers of personal information or anonymized information of data subjects in Japan subject to the PPC's reporting and improvement orders; clarify that the PPC can publish cases of offshore controllers who do not comply with such orders; and
- (Where a data subject can require the disclosure of details of data protection measures when his/her personal data is transferred to offshore transferees under the exception to the consent requirement due to implementation of data protection standards equivalent to the APPI (see question 9.1(c)(ii) above). Require a data controller to notify data subjects of the foreign country to which their data is transferred and give details of protection levels afforded by data protection laws in that country.

Comments from the public on the "Outline" were invited to be submitted until 14 January 2020.

The PPC has announced that (a) it will draft the bill of amendments to the APPI and aims to submit the bill to the ordinary Diet in 2020 (an ordinary Diet session is usually between January and June or July every year); and (b) amendments in the bill which require some time for the regulators, businesses and the public to prepare for will be implemented after such preparation period following implementation of the legislation.

12.3 What are some of the 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.

KENYA

1 PRIVACY LAW

1.1 How is privacy regulated in Kenya?

Currently, the law of privacy in Kenya is regulated by a layered legal framework which sets out the legal obligations, rights and remedies that apply to state bodies, public and private corporate enterprises and individuals. The fundamental right of privacy is primarily enshrined in the provisions of the Constitution of Kenya 2010 and in the provisions of the newly-enacted Data Protection Act 2019 ("DPA"), as well as various other acts, professional codes and court judgments. The DPA, which was assented to by the President of Kenya on November 11, 2019, and came into effect on November 25, 2019, intends to bring into effect the right of privacy as provided for in the Constitution by setting out the requirements for the protection of personal data processed by both public and private entities. The DPA also sets 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 will be binding on data controllers and data processors, whether public or private entities.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The general framework of statutes that caters to the protection of the right to privacy in Kenya comprises:

(a) Constitution of Kenya 2010 ("Constitution");

(b) Data Protection Act 2019; ("DPA");

(c) Access to Information Act No 3 of 2016;

(d) Computer Misuse and Cybercrimes Act No 5 of 2018 ("Computer Misuse Act");

(e) Kenya Information and Telecommunications Act No 2 of 1998 ("KICA");

(f) Official Secrets Act No 31 of 2016 ("OSA");

(g) HIV and AIDS Prevention and Control Act No 14 of 2006 ("AIDS Act");

(h) Kenya Information and Communication (Amendment) Bill 2019 ("Social Media Bill");

(i) Code of Advertising Practice and Direct Marketing by the Advertising Standards Body of Kenya ("CAP Code"); and

(j) Guidance Note on Cybersecurity by the Central Bank of Kenya, issued on August 2017 ("CBK Guidance").

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Both the Courts and sector-specific regulatory bodies such as the Office of the Data Protection Commissioner ("Commissioner") and the Communication Authority of Kenya enforce provisions of privacy law in Kenya. The DPA provides for the establishment of the Commissioner, whose functions will include overseeing the implementation and enforcement of the DPA, 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 DPA. Note that as at January 8, 2020, the Commissioner has yet to be appointed. We anticipate further updates on the establishment

of the office itself and the appointment of the Commissioner being announced in June or July 2020, however, this has not been confirmed. Until such time as the Commissioner is appointed, all privacy law-related matters will be resolved by the courts, and compliance with the DPA will be effectively self-regulated.

As regards any self-regulatory bodies, with the DPA still in its infancy, there are no self-regulatory bodies as such. As and when the Commissioner is appointed, one of the functions of the Commissioner will be to promote self regulation among data controllers and data processors.

2 SCOPE

2.1 Which companies are subject to privacy law in Kenya?

(a) The Constitution is binding on all State organs and all persons. Further, it provides that all persons have the right to privacy. The Constitution defines a "person" as 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 process personal data by automated or non-automated means. There are no residency requirements where the processing is done by automated means and the DPA therefore applies to foreign and local companies in this context. However, where personal data is processed by non-automated means, the DPA will apply only if the recorded data forms a whole or a part of a filing system by a data controller or data processor who:

(i) is established or ordinarily resident in Kenya and processes data while in Kenya, or

(ii) is not established or ordinarily resident in Kenya but who processes 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:

(i) giving effect to the Constitutional right to access information;

(ii) providing 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) providing a framework to facilitate access to information held by private bodies in compliance with any right protected by the Constitution and any other law.

The Act defines a "private body" to include any entity that receives public resources and benefits, utilizes public funds, engages in public functions, provides public services, has exclusive contracts to exploit natural resources or is in possession of information which is of significant public interest due to its relation to the protection of human rights, the environment or public health and safety, or to exposure of corruption or illegal actions or where the release of the information may assist in exercising or protecting any right.

2.2 Does privacy law in Kenya apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The DPA will apply to companies registered or otherwise located outside of Kenya that process personal data of data subjects located in Kenya. The Commissioner will prescribe the thresholds for mandatory registration by data controllers and data processors with the Commissioner, and registration with the Commissioner will apply to all companies, whether or not they have an establishment in Kenya.

The DPA provides that a data controller or data processor 'may' appoint a data protection officer; however, it is not yet clear whether this will be an absolute requirement imposed on data controllers and data processors not established or ordinarily resident in Kenya. The DPA places a particular emphasis on the designation of 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. That said, it is important to reiterate that the requirement to appoint a data protection officer is drafted as a discretionary obligation rather than a mandatory requirement.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Kenya?

(a) 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.

(b) Under the Access to Information Act, "personal information" is somewhat broader and is defined as:

(i) 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;

(ii) 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;

(iii) any identifying number, symbol or other particular assigned to the individual;

(iv) the fingerprints, blood type, address, telephone or other contact details of the individual;

(v) 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;

(vi) any information given in support of or in relation to an award or grant proposed to be given to another person; or

(vii) contact details of an individual.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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. The Commissioner may prescribe further categories of personal data which may classified as sensitive personal data at any time.

The DPA defines "biometric data" as 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.

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 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.

In the context of the transfer of any sensitive personal data, the consent of the data subject must be obtained prior to the 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.

In addition to the requirements under the DPA, the Health Act imposes confidentiality obligations regarding health data. It provides that information concerning a user, including information about his or her 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Companies must comply with the Data Protection Principles outlined in question 3.2.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The DPA applies equally to both data controllers and data processors; and both controllers and processors are required to register with the Commissioner.

The nature of the role will affect the reporting requirements that must be complied with in the event of a breach. The DPA requires the controller to notify and communicate the breach to the Commissioner and the data subject in the prescribed instances. However, a data processor is required to notify the data controller only, 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. This agreement must expressly provide that the data processor will act only on the instructions of the data controller and that the data processor agrees to be bound by the obligations of the data controller.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

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:

(a) to know how the information will be used;

(b) to access the data;

(c) to object to the processing of their data;

(d) to require the correction of false or misleading data; and

(e) to require the deletion of false or misleading data.

These rights must be upheld in addition to the Data Protection Principles highlighted in question 3.2.

The DPA requires there to be a lawful basis for the processing of personal data, and a data controller or data processor may not process personal data unless (i) the consent of the data subject has been obtained; or (ii) the processing is necessary for certain prescribed circumstances, including for the performance of a contract to which the data subject is party.

Regarding consent, the DPA allows for the withdrawal of consent at any time.

As to what amounts to "consent", the DPA follows generally internationally accepted standards in that the consent must be "express, unequivocal, free, specific and informed indication … by a statement or clear affirmative action". It is clear that a positive action from the data subject is required rather than

any form of deemed consent or requiring the data subject to withdraw their consent (eg, by way of an opt-out).

The law places particular emphasis on the need to obtain the consent of the data subject before disclosing information to third parties or transferring it outside the jurisdiction. A further requirement is to ensure that adequate security and technical mechanisms are in place to secure the information.

There are no legal requirements to implement privacy policies; however, a privacy policy is a mechanism by which companies can comply with their obligations under the DPA. The relevant obligations would include complying with the Data Protection Principles, notifying the data subject of his/her rights, complying with the duty to notify the data subject of certain requirements and informing the data subject of the manner in which it may object to processing.

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 format of an impact assessment will be prescribed by the Commissioner.

The appointment of a data protection officer and the requirement to register with the Commissioner have already been discussed above at question 2.2. Comprehensive recordkeeping of processing activities should form part of the internal processes of data controllers and data processors in order to ensure compliance with the DPA, particularly in the event of any audit carried out by the Commissioner as permitted under the DPA.

The DPA does not contain any specific provisions which relate to advertising; however, it does provide that personal data cannot be used for commercial purposes unless the express consent of the data subject has been obtained, or the data controller or data processor is authorized to do so under any written law and the data subject has been informed of this.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Kenya? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The DPA aims to provide unified regulation of data in Kenya. 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 the amount of personal data collected, the extent of the processing, the period of storage, the accessibility of such data, the cost of processing data and the technologies and tools used. Furthermore, as part of the registration process to be complied with under the DPA, the application to the Commissioner must include a general description of the risks, safeguards, security measures and mechanisms in place to ensure the protection of personal data.

It is worth highlighting that 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. For instance, the CBK Guidance requires regulated entities to have in place a cybersecurity strategy, governance charter policy and framework, which should be based on the institution's risk profile, size, complexity and nature of its business processes. It also requires that regulated entities maintain a current enterprise-wide knowledge base of their users, devices, applications and relationships with the customers. Furthermore, it requires that

institutions set up specific mechanisms to ensure that their data is protected. They must also conduct annual independent threat and vulnerability assessment tests to ensure they are prepared in the event of an unforeseen attack through cyber-crime.

6.2 How are data breaches regulated in Kenya? What are the requirements for responding to data breaches?

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.

The DPA requires data controllers or processors to communicate the breach to the Commissioner within 72 hours of becoming aware of the breach, and to communicate the breach to the data subject in writing within a reasonable period, unless the identity of the data subject cannot be traced. 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. 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 Commissioner as necessary for the purpose of preventing, detecting or investigating an offence by a concerned or relevant body.

The communication to the Commissioner 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 Commissioner or data subject require further information.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

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 protected 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 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 deletion of false or misleading data.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

As mentioned above, the DPA requires the data controller or processor to obtain the consent of the data subject before processing personal data for commercial purposes.

The data subject has the right to object to the processing of personal data (which can include any profiling to the extent necessary) for any commercial use. Where the data subject objects, their personal data cannot be processed for any commercial use.

The DPA provides that the Cabinet Secretary may, in consultation with the Commissioner, prepare a code of practice for the commercial use of personal data.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The use of any tracking technologies that generate location data of a data subject, 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). Aside from this, there are no express provisions or restrictions which prohibit or otherwise govern the use of tracking technologies under Kenyan law.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

As at the date of writing, Kenyan law does not have express laws on the regulation of targeted advertising and behavioral advertising. However, all targeted or behavioral advertising would have 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. The provisions of the CAP Code are aligned with the requirements under the DPA.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Kenyan law does not expressly provide for a required type of notice or consent in order to share data with third parties. The DPA simply requires that the data subject be notified of the intent to share his/her data with third parties and the safeguards adopted where data is transferred to a third party prior to collection. Additionally, personal data may be collected indirectly where the data subject has consented to the collection from another source.

8.5 Are there specific privacy rules governing data brokers?

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 commits an offense under 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 processors and data controllers are broad and would include data brokers in their ambit.

8.6 How is social media regulated from a privacy perspective?

Kenyan law does not have provisions on the regulation of social media companies. However, these companies have to ensure that users' right to privacy is protected under the Constitution. In addition, the Social Media Bill is still being considered by the legislature after its first reading in Parliament on October 2, 2019.

The Social Media Bill will, if passed, introduce stringent regulation of use of social media in the country. The Bill seeks to license social media companies by requiring them, among other things, to keep all the data of the users of their platforms and submit this to the Communications Authority of Kenya when required. As such, if the Social Media Bill is passed into law, there will be serious privacy implications for the rights of data subjects.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Although there is no specific regulation of loyalty programs and promotions from a privacy perspective, the DPA does apply where such programs collect personal data, and, in particular, sensitive personal data (which can include property details and marital details). In these circumstances, the information must be collected, processed and stored in accordance with the DPA. This would apply to any proposed commercial exploitation of any such data collected, which is restricted (see question 8.1 regarding the commercial use of data).

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The DPA does not bar the transfer of data outside Kenya. However, the 8th Data Protection Principle provides that 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 Commissioner of the appropriate safeguards with respect to security and protection of the personal data;

(b) it has given proof to the Commissioner of the appropriate safeguards, which include ensuring that the jurisdictions to which data is being transferred have commensurate data protection laws;

(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.

It is not clear whether all of the provisions under (a)–(c) must be satisfied and it is hoped that the Commissioner will clarify the requirements to be met for any cross-border data transfers. Until such time as the requirements have been clarified, we would recommend that parties ensure they comply with (a) or (b) and one of the sub-conditions under (c).

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. Until further guidance is issued by the Commissioner, the onus will be on the data controller or processor to show that appropriate safeguards are in place. The Commissioner 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 Commissioner is further entitled to prohibit, suspend or subject the transfer to such conditions as may be determined.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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 DPA does not address any issues that may arise from any intra-group transfers.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

(a) Under the Kenya Information and Communications Act

(i) Unauthorized access to a computer system: 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. The penalty upon conviction is 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) Unauthorized disclosure of a password: any person who knowingly discloses a password to access a computer system for unlawful gain commits an offence. The penalty is a fine not exceeding KES 200,000 (US $2,000) or imprisonment for a term not exceeding two years or both.

(b) Under the Data Protection Act

(i) Administrative Penalty: The maximum penalty that may be imposed by the Commissioner for an infringement of the DPA is KES 5 million (US $50,000) or, in the case of an undertaking, up to 1% of annual turnover, whichever is the lower.

(ii) General Penalty: Where a person commits an offense and no specific penalty has been provided, or otherwise contravenes the DPA, they may be liable to a fine not exceeding KES 3 million (US $30,000) or imprisonment to a term not exceeding 10 years or both.

In addition to the general penalty above, the Court may, to prevent a contravention continuing, order forfeiture of equipment used in committing the offense or prohibit any act related to the contravention.

(iii) Failure to comply with an enforcement notice: If a person is served with an enforcement notice, failure to comply is an offence. The maximum penalty that can be imposed is KES 5 million (US $50,000) or imprisonment to a term not exceeding two years or both.

(iv) Obstructing the Data Commissioner: It is an offense for any person to obstruct the Commissioner in the exercise of its powers, fail to provide information or assistance, deny entry to the Commissioner or give the Commissioner false or misleading information. The penalty upon conviction is a fine not exceeding KES 5 million (US $50,000) or imprisonment for a term not exceeding two years or both.

(v) Damage as a result of infringement of the DPA: 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.

(vi) Unlawful disclosure of personal data: 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.

(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. The penalty upon conviction is a fine not exceeding KES 100,000 (US $1,000) or imprisonment for a term not exceeding two years or both.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes. The law provides that individuals can institute actions for breach of privacy.

Under the Constitution, Article 22 provides that every person has the right to institute proceedings alleging the breach of constitutional rights. The High Court has jurisdiction over claims of infringement of the bill of rights in the Constitution. As such, if the right of privacy is infringed upon, one can institute a claim in the High Court. It is important to note that any party alleging the breach of constitutional rights should use a reasonable degree of precision in setting out the complaint, the provisions said to be infringed and the manner in which they are alleged to be infringed.

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.

Under the DPA, an individual can lodge a complaint with the Commissioner, which may investigate the complaint. Where the Commissioner 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Kenya which affect privacy?

There are currently no laws particular to Kenyan culture that affect privacy.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

(a) The Social Media Bill: The Social Media Bill seeks to introduce stringent regulation of the use of social media in the country. It seeks to license social media companies by, among other things, requiring them to keep all the data of the users of its platform and submit this to the Communications Authority of Kenya when required. As such, if this Bill is passed into law, there will be serious implications for the privacy rights of data subjects.

(b) The Data Protection Act: As indicated earlier (see question 1.3), we anticipate that the Commissioner will issue further regulations, guidance or codes in relation to the implementation and application of the DPA. The content of this guidance will not be subject to public debate and it is difficult to ascertain how prescriptive, prohibitive, liberal or restrictive this guidance will be.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Kenya?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Lately, there has been an increase in the number of Kenyans who have access to the internet. Accordingly, there has been a shift by Parliament towards increased regulation of information shared over automated platforms. The Kenyan government has also begun moving from manual storage of data to automated storage, with a view to achieving greater efficiency in the delivery of government services. However, the growing volumes of personal data that the government is collection have resulted in several court cases against it in relation to privacy protection.

12.2 What do you envision the privacy landscape will look like in 5 years?

Given the current trajectory of the landscape, we envision that privacy in Kenya will be subject to more regulation due to a growing appreciation of the need for regulation and protection of information. This will also bring about more certainty in terms of the rights and compliance obligations of data controllers and data processors. Additionally, access to internet and data services is expected to continue to grow, and we anticipate added growth in the number of companies offering ecommerce services.

12.3 What are some of the 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 European Union's General Data Protection Regulation, 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 which have the jurisdiction to determine 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. It is not yet clear what the extent of the enforcement actions to be taken by the Commissioner will be, but, with an increasingly aware population, companies should brace themselves for increased investigations and enforcements actions.

MALAYSIA

1 PRIVACY LAW

1.1 How is privacy regulated in Malaysia?

Personal data privacy is regulated under the Personal Data Protection Act 2010 ("PDPA").

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The primary source of law governing personal data privacy is the PDPA.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Privacy law is enforced by the Personal Data Protection Commissioner and by the public at large. Any individual or relevant person may make a complaint in writing to the Commissioner, 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 Commissioner may issue an enforcement notice outlining directions to be complied with by the data user.

2 SCOPE

2.1 Which companies are subject to privacy law in Malaysia?

Those that collect personal data to be processed or to be further processed in Malaysia.

2.2 Does privacy law in Malaysia apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 INFORMATION

3.1 How is personal information/personal data defined in Malaysia?

"Personal data" means any information in respect of commercial transaction, 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,

that relates directly or indirectly to a data subject, including any sensitive personal data and expression of opinion about the data subject.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive personal data" includes any personal data consisting of information as to the physical or mental health or condition of a data subject, his 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 him of any offence, or any other personal data as the Minister may determine by order published in the Gazette.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

There are seven principles that companies need to follow:

(a) General: A data user must not process personal data unless the data subject has given consent.

(b) Notice and Choice: A data user must, by notice in writing, inform a data subject:

  (i) that his/her personal data is being processed by or on behalf of the data user,

  (ii) the purpose for which the data is being or is to be collected and further processed, and

  (iii) the data subject's right to request access to and to request correction of his/her personal data.

(c) Disclosure: No personal data may, without the consent of the data subject, be disclosed for any purpose other than the purpose for which it was to be disclosed at the time of collection nor may it be disclosed to any party other than a third party known by the data subject.

(d) Security: A data user must, 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.

(e) Retention: The personal data processed for any purpose must not be kept longer than is necessary for the fulfilment of that purpose, and a data user has a duty to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

(f) Data Integrity: A data user must take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date, having regard to the purpose, including any directly-related purpose, for which the personal data was collected and further processed.

(g) Access: A data subject must be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under the PDPA.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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 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 a person who. either alone or jointly or in common with other persons. processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The law specifies that a data user must cease or not begin processing the personal data of a data subject for the purpose of communication by means of any advertising or marketing material if the data subject has notified the data user in writing of his/her wish not to have his/her personal data processed or further processed for such purposes.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Malaysia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is based on a standard of reasonableness. Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor:

(a) provides sufficient guarantees in respect of the technical and organization security measures governing the processing to be carried out; and

(b) takes reasonable steps to ensure compliance with those measures.

6.2 How are data breaches regulated in Malaysia? What are the requirements for responding to data breaches?

Data breaches are self-regulated. Any individual or relevant person may make a complaint in writing to the Commissioner, who will then investigate into 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 Commissioner may issue an enforcement notice outlining directions to be complied with by the data user.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

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 his/her 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 he/she knows that his/her personal data being held by the data user is inaccurate, incomplete, misleading or not up-to-date.

(c) Right to withdraw consent to process personal data: A data subject may by notice in writing withdraw his/her consent to the processing of his/her personal data.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

A data subject may, at any time, notify the data user, in writing, to cease or not to begin processing his/her personal data for marketing communications. If the data user fails to comply with the notice, the data subject may submit an application to the Commissioner to require the data user to comply with the notice. The Commissioner then may require the data user to comply with the notice. A data user who fails to comply with the Commissioner's requirement commits an offence and will, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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 the following good practices:

(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 be transferred to any party without prior approval from the data subject.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

N/A.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

N/A.

8.5 Are there specific privacy rules governing data brokers?

N/A.

8.6 How is social media regulated from a privacy perspective?

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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Transfer of personal data to a third party or places outside Malaysia must be done with the prior consent of the data subject. Additionally, a data user may transfer any 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

None.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

A data user who contravenes the personal data protection principles (see question 3.3) commits an offence and will, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

10.2 Do individuals have a private right of action? What are the potential remedies?

Private individuals have no private rights of action.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Malaysia which affect privacy?

None; except for religious or racial harmony.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

No, there are no imminent changes.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Malaysia?

No identification card or passport may be retained for any period — only for identification purposes.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

None.

12.2 What do you envision the privacy landscape will look like in 5 years?

What we foresee is the perverse implementation of facial and fingerprint scanning for private use.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The challenges for the future within the privacy landscape are the perverse use of artificial intelligence and surveillance of private individual.

MEXICO

1 PRIVACY LAW

1.1 How is privacy regulated in Mexico?

Privacy law is considered as a human right, according to the Federal Constitution. There are two main regulations on privacy in Mexico:

(a) The Mexican Data Privacy Law for the Private Sector ("Privacy Law"): this is an omnibus regulation and it has been in force since July 5, 2010; and

(b) The General Data Protection Law for the Public Sector ("Public Sector Data Law") has been in force since January 26, 2017: this is also a general regulation addressed at government agencies processing personal data; however, as this is a general regulation, it only sets the standards for data processing, and each state has its local data protection law for public sector.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Currently, the Mexican data privacy regulation is based on the following laws:

(a) The Federal Constitution recognizes data privacy as a human right (Articles 6 and 16);

(b) The Privacy Law;

(c) The Rules for the Privacy Law ("Rules");

(d) The Consumers Protection Law (the only regulation focusing on advertising aspects, where it is stated that suppliers should provide an adequate use of personal data, according to privacy laws);

(e) The Public Sector Data Law;

(f) Local regulations, eg the Civil Liability, Honor and Private Life Act (applicable for Mexico City, only);

(g) Mexico is the second Latin American country to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as "Convention 108", and its Additional Protocol, and thus becomes its 53rd Party; and

(h) Mexico is also a member party of the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The data protection authority in Mexico is the Mexican Institute of Transparency and Personal Data Protection ("INAI") and it is the authority in charge of:

(a) transparency and access to public information; and

(b) personal data protection.

The INAI is a constitutional and autonomous entity, it has enough capacities to enforce the law without meddling from other governmental entities.

2 SCOPE

2.1 Which companies are subject to privacy law in Mexico?

Those regulated by privacy law in Mexico are private individuals and legal entities that carry out the processing of personal data, with the exception of:

(a) Credit information societies (in the case of the Law to Regulate Credit Information Societies and other applicable provisions), and

(b) persons who carry out the collection and storage of personal data which is for personal use only, and without purposes of disclosure or commercial use.

2.2 Does privacy law in Mexico apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Mexico?

"Personal data" is defined as any information concerning an identified or identifiable natural person.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" refers to personal data that affects the most intimate sphere of its owner, or improper use of which may cause discrimination or carries a serious risk for an individual. In particular, sensitive data is that which may reveal aspects such as:

(a) racial or ethnic origin,

(b) present and future state of health,

(c) genetic information,

(d) religious, philosophical and moral beliefs,

(e) trade union membership,

(f) political opinions, and

(g) sexual preference.

A specific obligation around sensitive data is that explicit and written (electronic means are allowed) consent of individuals must be obtained prior to the data processing (sensitive data is based on the opt-in system; other personal data is based on the opt-out system).

Also, fines for data processing infringement can be doubled when it comes to sensitive data.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The principles that govern data privacy in Mexico are:

(a) lawfulness,

(b) consent,

(c) information,

(d) quality,

(e) purpose,

(f) loyalty,

(g) proportionality and

(h) responsibility.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Yes, the Mexican Privacy Law assigns different roles to subjects based on how they process personal data. There are two roles:

- **Controller** is an individual or legal entity of a private nature who decides on the processing of personal data.
- **Processor**: is an individual or legal entity who alone or jointly with other persons processes personal data on behalf of the controller.

The controller and processor should sign a contract, or at least include a clause in their service agreement, in order to set out minimum standards on processing personal data, including security standards. The agreements between the controller and processor relating to processing must be in accordance with the relevant privacy notice.

The processor has the following obligations in respect of processing carried out on behalf of the controller:

(a) process personal data only in accordance with the instructions of the controller;

(b) refrain from processing personal data for purposes other than those instructed by the controller;

(c) implement security measures in accordance with the Privacy Law, its Rules and other applicable provisions;

(d) keep personal data confidential;

(e) delete the personal data subject to processing once the legal relationship with the controller has come to an end, or on the instructions of the data controller, provided that there is no legal provision requiring the conservation of personal data; and

(f) refrain from transferring personal data unless either the controller so instructs, the communication derives from subcontracting, or when so required by the competent authority.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Key obligations are:

(a) obtaining consumer's consent prior to data processing;

(b) posting a privacy policy prior to data processing;

(c) appointing a data privacy officer;

(d) complying with the so-called "ARCO rights" (ie, the data subject's rights of Access, Rectification, Cancellation and Opposition); and

(e) complying with the principles for data processing (see question 3.3).

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Mexico? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The law requires controllers to take technical and physical security measures to protect personal data against breach, loss, alteration, destruction or use, access or unauthorized processing.

6.2 How are data breaches regulated in Mexico? What are the requirements for responding to data breaches?

In the event of any data breach, the controller must inform the data subject without delay, when there is a risk of his/her right to privacy being infringed, so he/she can take the necessary actions.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals have ARCO rights: ie, Access, Rectification, Cancellation and Opposition. Currently, the right to data portability is only applicable for the Public Sector Data Law.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communication is allowed under the Privacy Law, as long as the data subject is informed prior to data processing. Spam is forbidden under the Consumers Protection Law.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Controllers are obliged to inform data subjects when using tracking technologies, as part of the Information Principle (see question 3.3).

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Controllers are obliged to inform data subjects when they are using targeted advertising and behavioral advertising, as a part of the Information Principle (see question 3.3).

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

A privacy notice should indicate that the controller is transferring personal data to third parties and for what purposes.

8.5 Are there specific privacy rules governing data brokers?

No.

8.6 How is social media regulated from a privacy perspective?

There are no specific regulations on social media in the Privacy Law, other than that social media can be considered as a public access source. In the public sector, there are recent judgments issued by Federal courts stating that public officers may not block users, as this is inhibiting the right of information access.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are no specific regulations for loyalty programs, although there are some specify provisions regarding promotions in the Privacy Law and the Consumers Protection Law.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

National or international data transfers (other than to a processor) may only be carried out if the data subject gives his/her consent and the controller must provide the third party with the privacy notice relevant to the data subject and inform the third party as to the purposes for which the data may be processed to which the data subject has consented. The third-party recipient must meet the same minimum-security standards as are required from controllers. See question 4.1 as to the requirements on processors.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

No consent is required when transferring data between group companies.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

For violations of privacy or data security law, the law provides a list of actions that are grounds for sanction. Fines from 100 to 320,000 times the current minimum daily wage (approximately US $5.38 a day) may be imposed, and may be doubled when it comes to sensitive data.

Sanctions may be imposed without prejudice to any civil or criminal liability that can arise.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes, individuals have right of actions when the Privacy Law is infringed. According to article 58 of the Privacy Law, individuals who consider that they have suffered damage or injury to their property or rights as a result of non-compliance with the provisions of the Privacy Law by the controller or processor may bring actions for compensatory damages in a Federal court.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Mexico which affect privacy?

Privacy is regulated locally in each of the states of Mexico through the civil law, whereby individuals may pursue civil liability actions.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

- The Fintech Law, which came into effect on March 10, 2018, is intended to build a regulatory framework aimed at the development of innovative financial services, increasing the level of competition and financial inclusion, as well as placing Mexico at the forefront of the industry. The Fintech Law currently recognizes two types of financial technology institutions (crowdfunding institutions and electronic money institutions) and an innovative, or sandbox, model.
- In 2019, a set of Official Standards for e-commerce platforms was enacted. These standards require e-commerce platforms to comply with privacy regulations.
- In the upcoming months a regulation on drones will be drafted.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Mexico?

In Mexico, the burden of proof lies on controllers.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

In 2019, 13 out of 32 states in Mexico passed the General Law on Women's Access to a Life Free of Violence; these local laws criminalize revenge porn, grooming, and sexting, among other matters. Some of these states which have passed this law are: Jalisco, Puebla, Oaxaca, Chiapas, Veracruz, and Yucatan; the City of Mexico is currently analyzing this law.

The trigger for this law is the urgent need to criminalize a very common practice on the internet, namely the sharing of explicit videos and photographs depicting sex on social media and posting them on porn sites.

12.2 What do you envision the privacy landscape will look like in 5 years?

- More international cooperation;
- Mexican framework needs to improve mechanisms to protect children's online privacy.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

One major challenge companies face is the cost of implementing a privacy policy according to local (national) frameworks.

NEW ZEALAND

1 PRIVACY LAW

1.1 How is privacy 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 1993 ("Privacy Act"). Self-regulatory frameworks including, eg, the Advertising Standards Authority's codes, also regulate privacy to a certain degree.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The key law regulating privacy is the Privacy Act. The Privacy Act sets out privacy principles which are the key principles that companies need to follow, as further detailed at question 3.3. 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 2013;

(b) Credit Reporting Privacy Code 2004;

(c) Health Information Privacy Code 1994;

(d) Justice Sector Unique Identifier Code 1998;

(e) Superannuation Schemes Unique Identifier 1995; and

(f) Telecommunications Information Privacy Code 2003.

There are also self-regulatory frameworks which regulate privacy, including the New Zealand Advertising Standards Authority ("ASA") and its advertising codes.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The provisions of the Privacy Act and associated codes are enforced by the Privacy Commissioner. A decision of the Privacy Commissioner can be appealed to the Human Rights Review Tribunal, which is an independent judicial body, separate from the office of the Privacy Commissioner. A breach of the privacy provisions contained in the ASA's codes is enforced by the ASA.

2 SCOPE

2.1 Which companies are subject to privacy law in New Zealand?

The Privacy Act applies to "agencies" that are defined as "any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department."

2.2 Does privacy law in New Zealand apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, if they operate in New Zealand. There are no specific requirements applicable only to overseas companies.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 in relation to sensitive information. However, codes of practice that the Privacy Commissioner issues, referred to above at question 1.2, are examples of areas where there are specific privacy requirements. For example, the Health Information Privacy Code sets out rules for the health sector.

The ASA recognizes the sensitivity of personal information relating to children in its Children and Young People'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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The Privacy Act sets out privacy principles which are the key principles that companies need to follow. A summary of the principles is set out below.

(a) Collection: Personal information can only be collected for lawful purposes, and its collection must be necessary for that purpose. 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:

(i) the information is being collected;

(ii) the purpose for which the information is being collected;

(iii) the intended recipients of the information;

(iv) the name and address of the entity that is collecting the information and the entity that will hold the information;

(v) if the information is authorized or required by law, details of this;

(vi) the consequences (if any) if all or any part of the information is not provided; and

(vii) 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.

(b) Storage of Personal Information: Personal information must be protected, by such safeguards as are reasonable in the circumstances, against loss, access, use, modification or unauthorized disclosure and other misuse.

(c) Access to and 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 entity holding personal information should not use that information without taking all reasonable steps in the circumstances, to ensure that, having regard to the purpose for which the information may be used, the information is accurate, up to date, complete, relevant and not misleading.

(d) Retention: Personal information should only be held for the time period required for the purpose for which it may be lawfully used.

(e) Use: Personal information may only be used for the purpose for which the individual was advised it was collected for. 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.

(f) 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.

(g) Unique Identifiers: An entity 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 entity must also not assign a unique identifier to an individual, unless it is required to enable the entity to carry out one or more of its functions efficiently.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No, the Privacy Act does not assign different roles to companies based on how they process information.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The key obligations under the Privacy Act are compliance with the privacy principles, set out at question 3.3. In addition, the Privacy Act requires that each organization has at least one Privacy Officer. The responsibilities of a Privacy Officer include, encouraging compliance with the privacy principles, dealing with any requests made under the Privacy Act, working with the Privacy Commissioner in relation to any investigations and otherwise ensuring compliance by the organization with the Privacy Act.

The privacy principles require that organizations inform individuals about information that is being collected and the purpose for which it is used, amongst other things. This is normally contained in a privacy policy or privacy statement.

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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in New Zealand? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is primarily regulated by the Privacy Act and its information privacy principles. As mentioned above at question 3.3, 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:

(a) the information is protected by such security safeguards as it is reasonable in the circumstances to take against:

  (i) loss;

  (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information;

  (iii) other misuse; and

(b) 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.

As referred to above, 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.

Further, the codes of practice issued by the Privacy Commissioner impose additional obligations regarding securing data for certain classes of agencies, such as credit reporters and telecommunications providers.

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 practices, such as:

(a) ISO/IEC 27001:2013 standard — This standard 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.

(b) The Protective Security Requirements ("PSR") — The PSR outlines the Government's expectations for managing personnel, physical and information security. The PSR also includes 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.

(c) 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.

6.2 How are data breaches regulated in New Zealand? What are the requirements for responding to data breaches?

Data breaches are regulated by the Privacy Act. Currently, the Privacy Act does not contain mandatory breach reporting requirements. However, this is under review as part of the review of the Privacy Act, as further discussed below.

The Privacy Commissioner recommends that the following steps are taken by an affected organization as quickly as possible to minimize any harm to the affected individuals and the organization concerned:

(a) Contain the breach and make a first assessment — This may include stopping unauthorized practices, retrieving lost information, disabling the breached system, cancelling or changing computer access codes and fixing weaknesses in the organization's physical/electronic security. It may also be necessary to consider whether to inform the organization's insurer, internal auditors, risk managers and legal advisers (and if the breach involves theft or criminal activity, notify the police and retain key evidence).

(b) Evaluate the risks — The organization should consider the types of personal information involved, what that information might show, how easy it is to hack, the cause, extent and potential harm of the breach and who holds the information.

(c) Notify affected people — The requirements and extent of notification is currently considered on a case by case basis. If there is no harm, notification may not be necessary.

(d) Prevent a repeat — This is intended as a longer-term solution to develop prevention strategies and could be affected by organizations establishing a comprehensive security plan for all personal information. The Privacy Commissioner recommends the International Organization for Standardization standards as a starting point. Further, organizations may, depending on the significance of the breach, need to undertake a security audit and review their policies and practices.

The Privacy Act is currently undergoing review. A new Privacy Bill ("Privacy Bill") was introduced in 2018 and is expected to be enacted into law in 2020. One of the key proposed changes to the Privacy Act is mandatory data breach notification, which will require public and private sector agencies to notify affected individuals and the Privacy Commissioner if they experience a data breach which poses a risk of harm. Failure to do so could result in a fine of up to NZ $10,000.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The privacy principles mentioned above at question 3.3 under the Privacy Act must be followed by businesses 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.

In the event of a breach of any of the information privacy principles or other provisions of the Privacy Act, the individual concerned can make a complaint to the Privacy Commissioner who will be responsible for investigating the breach. As mentioned at question 6.2, under the new Privacy Bill it is proposed that businesses will be required to notify affected individuals and the Privacy Commissioner if they experience a data breach which poses a risk of harm, and failure to do so could result in a fine of up to NZ $10,000. Further, if a privacy breach matter is not settled with the Privacy Commissioner, then the decision can be appealed to the Human Rights Review Tribunal.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The Privacy Act primarily regulates 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

In addition to the information privacy principles under the Privacy Act regarding collection, purpose, and disclosure (if any) of personal information, rule 1(b) of 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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

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 in the private sector. As a result, data matching in the private sector is, for the most part, regulated by the 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). 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.

8.5 Are there specific privacy rules governing data brokers?

Currently, 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.

8.6 How is social media regulated from a privacy perspective?

Social media 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 or emails, social media platforms will be subject to the provisions of the Unsolicited Electronic Messages Act 2007 as referred to above in response to question 8.1.

Otherwise, social media remains relatively unregulated from a privacy perspective in New Zealand. However, in recognition of changes in the use of data, the Privacy Commissioner has submitted a substantial set of recommendations for the Privacy Bill, some of which will impact directly on the use of personal information by social media platforms. These include:

(a) right to erasure,

(b) fair use of personal information,

(c) algorithmic transparency (openness about the purpose, structure and underlying actions of algorithms used to manipulate data) and

(d) recommendations in relation to mandatory breach notifications and penalties for serious non-compliance.

Further, the Privacy Commissioner could be given 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.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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, ie, beyond completion of the program or promotional offer.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The handling of "personal information" (as defined in the Privacy Act) must comply with the Privacy Act's privacy principles (see question 3.3). An organization must not transfer personal information to another organization except in compliance with the privacy principles. The Privacy Commissioner may issue a transfer prohibition notice under Section 114D of the Privacy Act, prohibiting the transfer of personal information as set out in the notice.

The current version of the Privacy Bill prohibits the disclosure of personal information overseas unless an agency can be satisfied of one of the set criteria (eg, that the foreign person receiving the personal information is subject to privacy laws that, overall, provide comparable safeguards to those in the Bill) is satisfied.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

The Privacy Bill proposes that a company (acting as an agent for another) that is storing or processing information for another company that uses or discloses information for its own purposes will be held accountable and treated as holding the information (even if that company is not situated in New Zealand), for example, cloud data storage providers and information sent overseas for processing on behalf of an agency, in certain circumstances. Similarly, a company will remain accountable for the information held by another person as its agent.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

If there is a breach of one or more privacy principles, the affected 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. The Tribunal has awarded up to NZ $10,000 for less serious breaches and up to NZ $50,000 for more serious breaches. The greatest award the Tribunal has ordered in respect of a privacy matter was over NZ $168,000. The Tribunal has the ability to award damages up to NZ $350,000.

Further, a person commits an offence under the Privacy Act and is liable upon conviction for up to NZ $2,000 for:

(a) obstructing or not complying with the Privacy Commissioner in the exercise its power under the Privacy Act;

(b) knowingly misleading the Commissioner to exercise its powers under the Privacy Act; or

(c) misrepresenting their authority under the Privacy Act.

The current version of the Privacy Bill raises the maximum liability for the above offences to NZ $10,000 and creates new offences, including:

(d) misleading an agency to obtain access to someone else's personal information; and

(e) destroying a document containing personal information, knowing a request has been made for it.

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 individuals have a private right of action? What are the potential remedies?

Individuals may bring a common law claim for an invasion of privacy.

Individuals can seek an injunction to prevent invasion of their privacy.

General damages (for example, compensation for hurt and upset) and exemplary damages are also available as remedies.

As referred to above, an individual personally affected by the breach (or that individual's representative) may make a complaint to the Privacy Commissioner.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of New Zealand which affect privacy?

There are no specific privacy rules which relate to the culture of New Zealand.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

As discussed at question 6.2, the Privacy Act is currently under review. All companies that collect, store and use personal information about their employees and/or customers will need to be aware of the changes the Privacy Bill makes to New Zealand's current privacy law. Key changes include mandatory reporting requirements with respect to certain data breaches and the strengthening of cross-border data flow protection.

11.3 **Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in New Zealand?**

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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

Since its introduction of the Privacy Act, the Privacy Act has continued to act as the primary source of legislation for addressing privacy and data issues in New Zealand. The legislation adopts a principle-based approach, has been drafted on a technologically neutral basis, and has remained relatively unchanged since its original enactment. However, as detailed in question 12.2, a significant revision of the privacy regime is currently under discussion in the New Zealand Parliament. This reform is likely a response to the advancement and proliferation of the digital economy which has significantly altered the privacy landscape.

12.2 What do you envision the privacy landscape will look like in 5 years?

As noted at question 6.2, the Privacy Bill will strengthen privacy protections, focusing on early intervention and risk management by those who hold or handle personal information. The current version of the Privacy Bill proposes key reforms:

(a) Mandatory reporting requirements — agencies are required to report to the Privacy Commissioner and the individual concerned where there has been a privacy breach which poses a risk of harm.

(b) Greater scope of powers for the Privacy Commissioner — the Privacy Bill in its current form gives the Privacy Commissioner more information-gathering powers, the authority to issue "Compliance Notices" (which require an agency to do or stop something) and the ability to make binding decisions on complaints in relation to the access of information under the Privacy Act.

(c) Cross-border protections — In light of the ease of data flowing between jurisdictions, to promote accountability and satisfactory protections of the personal information of New Zealand individuals, New Zealand agencies will be required to be satisfied that any personal data it sends overseas will be protected by equivalent or better privacy standards.

(d) Penalties — in recognition of the importance of privacy protection, the enactment of the Privacy Bill in its current form will introduce various new penalties and heavier fines (see question 10.1).

12.3 What are some of the 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.

NICARAGUA

1 PRIVACY LAW

1.1 How is privacy 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 21 March 2012 and came into effect upon publication in the Official Journal on 29 March 2012.

This law regulates the processing of personal data relating to both natural persons and legal entities regardless of whether it is carried out by automated means or not. The objective of this law, as stated in Article 1, is to guarantee the right to personal and family privacy, as well as the right to information self-determination.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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, at the present time, the Directorate has not yet been created, and, therefore, the Law is not fully applicable, as it is not possible to comply with certain requirements of the law, such as registering in the Directorate's database. Furthermore, it is not possible to impose administrative sanctions (in cases of violations) and there is currently no entity in charge of monitoring compliance.

2 SCOPE

2.1 Which companies are subject to privacy law in Nicaragua?

Both public entities and private companies are subject to the Nicaraguan privacy law.

2.2 Does privacy law in Nicaragua apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No. There is no explicit mention of the territorial scope of the Law on the Protection of Personal Data, which, by default, limits its scope of application to entities established in the Nicaraguan territory processing data contained in databases kept within Nicaragua.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Nicaragua?

"Personal data" is defined as any information relating to an identified or identifiable natural persons or legal entities.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

(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 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 abuses. As a result, the entity collecting the data must take appropriate technical measures to prevent any unauthorized access 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.

(g) Accountability: Data subjects should have a method available to them to hold data collectors accountable for following the principles outlined above.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No. The law in Nicaragua does not assign different roles to companies based on how they process personal data.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

(a) The Law on the Protection of Personal Data requires:

(i) Posting a privacy policy in local language (Spanish).

(ii) Registering with the Directorate for Persona Data Protection (when such Directorate has been established — see question 1.3).

(b) Additionally, the Law on the Protection of Rights of Consumers and Users (Law No 842) broadly defines advertising as: "all form of public communication made by a provider for promoting directly or indirectly the acquisition of goods and/or services is considered advertising." This includes the action of sending marketing e-mails and text messages.

The following general principles should be followed:

(i) The communications must offer the right to opt out of future communications or to revoke consent.

(ii) The communications (advertising) must be free from false or misleading information.

(iii) Unless the information has been obtained from publicly available sources, all personal information maintained in direct marketing databases can only be included with the consent of the individuals concerned. In any case, these individuals have the right to access their information stored in such databases.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Nicaragua? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is also regulated by the Law on the Protection of Personal Data.

This Law 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, in view that said directorate has yet to be created, there are no particular standards in place for securing data.

6.2 How are data breaches regulated in Nicaragua? What are the requirements for responding to data breaches?

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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications may only incorporate personal data with the consent of the owner or unless the data was obtained from sources accessible to the general public.

The owner of the data may exercise the right of access without charge, and may, at any time, request the deletion of its 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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Advertisers should provide notice to the data's owners, informing them that the data is to be shared and the purpose of doing so.

8.5 Are there specific privacy rules governing data brokers?

Data brokers must:

(a) take the necessary safety measures;

(b) keep data confidential; and

(c) obtain registration.

8.6 How is social media regulated from a privacy perspective?

Our Law on Protection of Personal Data provides that owners of the personal data have the right to request social networks, browsers and servers to delete and cancel any of their personal data found in their files.

In the case of data files of public and private institutions that offer goods and services and that for contractual reasons collect personal data, once the contractual relationship is terminated, the owners of the data may request that all personal information be deleted.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

According to the Law on the Protection of Personal Data, the owners of the personal data should be informed of their rights over such data, the origin of the data and the entity responsible for the handling of the same. The personal data can only be incorporated with the owner's consent unless it was obtained from sources accessible to the general public.

The owners of the data may exercise the right of access without charge, and may, at any time, request the deletion of their data files.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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 (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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Not at present.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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.

(c) Compensation of damages.

10.2 Do individuals have a private right of action? What are the potential remedies?

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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Nicaragua which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Not currently.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Nicaragua?

Not currently.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

In Nicaragua, the privacy landscape has not changed over the past few years. Although the Law on the Protection of Personal Data has been in force since 2012, the regulatory authority (Directorate of Personal Data Protection) has yet to be created. As a result, the law is not entirely enforceable.

12.2 What do you envision the privacy landscape will look like in 5 years?

There is some expectation that at some point the regulatory authority (Directorate of Personal Data Protection) will be created.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

At present, there are no regulations in place because the regulatory authority has yet to be created. However, once created, companies will need to pay close attention to the regulations being drafted.

NIGERIA

1 PRIVACY LAW

1.1 How is privacy 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) provides protection for the right to private life under its Section 37. The Nigerian Legislature has also passed the Nigeria Data Protection Regulations 2019 ("NDPR"). These Regulations were issued by the National Information Technology Development Agency ("NTDIA") on January 25, 2019, pursuant to the National Information Technology Development Agency Act 2007.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The NDPR is the most relevant law which deals with data protection and privacy.

Other laws which contain limited provisions on privacy are:

(a) The Constitution Federal Republic of Nigeria 1999 (as amended in 2011);

(b) National Information Technology Development Agency Act 2007;

(c) Freedom of Information Act 2011;

(d) Nigerian Communications Act 2003;

(e) Child Rights Act 2003;

(f) Cybercrimes (Prohibition, Prevention Etc) Act 2015;

(g) National Identity Management Commission Act 2007;

(h) Consumer Code of Practice Regulations 2007;

(i) Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011;

(j) Consumer Protection Framework 2016;

(k) The Credit Reporting Act 2017; and

(l) The National Health Act 2014.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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 same. However, privacy laws in Nigeria may be enforced through a civil action in a High Court by relying on Sections 37 and 45 of the 1999 Constitution.

The NITDA is also responsible for setting up an Administrative Redress Panel whose duty it is to investigate allegations of breach of privacy, conclude its investigations and determine, within 28 days, the appropriate redress.

2 SCOPE

2.1 Which companies are subject to privacy law in Nigeria?

All companies in Nigeria are subject to privacy law.

2.2 Does privacy law in Nigeria apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Only the NDPR apply to businesses established in other jurisdictions. According to the NDPR, they 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 INFORMATION

3.1 How is personal information/personal data defined 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, IMEI number, IMSI number, SIM and others.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive personal data" refers to 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The NDPR provides 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 his or her 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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No. The NDPR 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 this regulation, relevant data privacy instruments and data protection directives of the data controller, provided that 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 data processing, etc.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

There are no specific requirements under the privacy laws for data protection with respect to advertising.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Nigeria? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

In Nigeria, anyone involved in data processing or the control of data must develop security measures to protect data; such measures include, but are not limited to:

(a) protecting systems from hackers,

(b) setting up firewalls,

(c) storing data securely with access to specific authorized individuals,

(d) employing data encryption technologies,

(e) developing an organizational policy for handling personal data (and other sensitive or confidential data),

(f) protection of emailing systems, and

(g) continuous capacity building for staff.

Any person engaging a third party to process the data obtained from data subjects must ensure adherence to the NDPR and to the measures indicated above.

6.2 How are data breaches regulated in Nigeria? What are the requirements for responding to data breaches?

Data breaches are regulated through sanctions specified under the NDPR.

There are no specific requirements for responding to data breaches.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals have the following rights:

(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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

No specific regulations exist in this regard.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There are no specific regulations in this regard.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There are no specific regulations in this regard.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

There are no specific regulations in this regard.

8.5 Are there specific privacy rules governing data brokers?

There are no specific regulations in this regard.

8.6 How is social media regulated from a privacy perspective?

There are no specific regulations in this regard. Although the Federal Government attempted, in 2019, to regulate social media (through the Digital Rights Bill, the National Commission for the Prohibition of Hate Speeches (Est etc) Bill, 2019 and the Protection from Internet Falsehoods and Manipulations and Other Related Matters Bill 2019), these Bills are still undergoing reading at the National Assembly, and have not yet been passed.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

No specific regulations in this regard.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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 NTDIA 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 case-law 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

In the absence of any decision by the NTDIA or the Attorney General as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of personal data to a foreign country or an international organization may take place only on 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 are likely to be violated in the event of transfer to a third country. This proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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, payment of the fine of 2% of annual gross revenue of the preceding year or payment of the sum of 10 million naira whichever is greater;

(b) in the case of a data controller dealing with less than 10,000 data subjects, payment of the fine of 1% of the annual gross revenue of the preceding year or payment of the sum of 2 million naira whichever is greater.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes. Individuals may claim damages as compensation in a civil suit.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Nigeria which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

None.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Nigeria?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

No particular changes have occurred, as a consequence of the fact that privacy laws in Nigeria have not really developed.

12.2 What do you envision the privacy landscape will look like in 5 years?

Relatively the same.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Foremost of these challenges is the pace at which privacy laws develop in Nigeria.

NORWAY

1 PRIVACY LAW

1.1 How is privacy 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") article 6(1)(f)).

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 will try to interpret national provisions in such a way to avoid conflict with EU law to the extent possible.

For communications, the ePrivacy Directive is substantially implemented through the Norwegian Act relating to Electronic Communications of 2003.

The Norwegian Personal Data Act has several provisions in addition to the GDPR. Some of these provisions will be part of the answers below.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

As mentioned above, the main framework consists of the Constitution, the GDPR 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.

(b) Employment: An employer is entitled to access to employees' emails or other private files when there is reason to believe that information in the individual's work email account is necessary for operational purposes.

An employer may also access such data when the employee is suspected of gross breach of duty. 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: In addition, detailed security requirements are often found in regulations and widely used standard agreements required by the government.

(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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

There are several supervisory authorities which enforce privacy rules:

(a) the National Communications Authority enforces the Electronic Communications Code which implements the ePrivacy Directive;

(b) the National Data Protection Authority ("DPA") enforces the Norwegian Personal Data Code which implements the GDPR; and

(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 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

See the European Union chapter.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Norway?

See the European Union chapter.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter.

While not formally considered as special categories of personal data (in terms of the GDPR article 9), 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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter. In Norway, the DPA currently seems to be specially interested in security and privacy by design and default.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter. The concepts of "controllers" and "processors" are the same.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Norway? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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 access 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.

The DPA has an ombudsman role for issues relating to personal data. It is to provide advice and information. This is done, amongst others, by means of guidelines and information published on its website.

6.2 How are data breaches regulated in Norway? What are the requirements for responding to data breaches?

See the European Union chapter.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

The Norwegian Personal Data Code 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 Code 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

As mentioned in question 1.2, the Marketing Act requires consent for most marketing communication done by enterprises, such as email and automated calls.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

In addition to the GDPR, the ePrivacy Directive is also substantially incorporated into Norwegian legislation, being written into the Act relating to Electronic Communications of 2003. Consent is explicitly required for cookies. The wording of the Code is not unambiguous as regards tracking, other than that based on placing information on the end user device. As some pixels, in addition to other technology, place data on the end-user device, such pixels are within the ambit of the Code. Tracking and SDKs which solely process software or hardware data — such as browser fingerprinting — is not as clearly within the ambit of the Code as traditional cookies. However, such tracking and SDKs would, in most cases, likely be subject to the GDPR because of their level of detail.

The consent requirement in the Electronic Communications Code deviates from that in the GDPR. The distinction is elaborated in the Act's preparatory works. In the preparatory works it is stated that general internet browser consent is valid. Even though the ECJ has concluded that active consent from the data subject is required, the Norwegian communications authority seems to conclude otherwise. Likely reasons for this divergence are the preparatory works and that fact that Norway is not an EU Member state.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter and question 8.2.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

Norway has decided that data subjects who are 13 years or older can consent to information society services.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

In addition, there are some rules which are specific to Norway. If more than 5 years have elapsed after a breach of the law, the DPA may not fine the controller or processor, unless the DPA finds that there is an ongoing case. Also, in addition to fines, the DPA may impose liquidated damages for every day the controller or processor fails to act as ordered by the DPA.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

Individuals can file a complaint anonymously to the DPA. Individuals can also claim damages — even if the individual has not suffered any economic loss.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Norway which affect privacy?

Norwegian culture is privacy-oriented in comparison to several other cultures. Post GDPR, Norway is one of the countries with the strictest privacy rules. In some cases, the previous rules were stricter than the GDPR.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The Norwegian Consumer Council recently filed a complaint with the DPA against several Ad-tech companies. In addition, the Norwegian Consumer Council states that they assess several current Ad-tech solutions to be threats to privacy and, in a broader sense, society.

The lawmakers are currently assessing framework legislation to ensure IT security.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Norway?

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 of 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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

The authorities are more interested in all forms of digital tracking than before. This is mainly triggered by public debate.

The authorities also focus more on apps than before. This is likely propelled by several security breaches.

Data subjects are far more aware of their privacy rights; this is likely because "GDPR" has been a big buzzword in Norway.

12.2 What do you envision the privacy landscape will look like in 5 years?

As technology advances, it could mean less privacy in practice. On the other hand, privacy by design and default is frequently requested in public tenders, and private actors frequently also require this. Consumers are also increasingly interested in such designs.

The DPAs seems to be tightening its grip, which will drive controllers and processors to comply. DPA cases and breaches could also seriously harm goodwill.

When speaking of data, authorities are increasingly assessing giants such as Google and Facebook as rivals. Over time this could decrease Google and Facebook's influence.

Though I am probably in the minority in thinking so, I think privacy in Norway (and probably Europe) will be enhanced over the next five years. Technology will advance — but technology already has enormous potential for being intrusive. Privacy rules, on the other hand, are gaining far more traction than before. The main question is whether the rules will move from the books to practice.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Data driven companies probably face the biggest challenges. Some of these need to reassess their core business model.

Other companies don't need to reassess their core business, but, surprisingly, many need to get a far better overview of what data they have; secure it; and comply better.

PANAMA

1 PRIVACY LAW

1.1 How is privacy regulated in Panama?

Privacy data matters in Panama are regulated by:

(a) the Political Constitution;

(b) legal provisions included in different laws and codes; and

(c) international conventions ratified by Panama.

Personal data will be regulated by Law No 81 of March 26, 2019 About the Protection of Personal Data ("Law No 81").

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) The key law regulating personal data matters is Law No 81, which will become effective on March 26, 2021. Implementing regulations are pending. This law provides definitions for confidential data, sensitive data and personal data.

(b) The Political Constitution of the Republic of Panama also contemplates the right of privacy in several of its provisions.

(c) The Family Code contains the obligation of the State in providing the necessary protection for privacy and ratifies the norm that requests previous authorization for the revelation of information of the persons.

(d) The Judicial Code establishes that personal information may only be shown to the interested party and prohibits the sharing of the same with other persons.

(e) The Republic of Panama has subscribed to various International Conventions in connection with the right of privacy, including the International Covenant on Civil and Political Rights.

(f) Special laws provide special protection to the right of privacy, including, among others:

  (i) Law No 26 of December 17, 1992, which protects the identity and information related to patients infected with the HIV virus,

  (ii) Law No 13 of July 27, 1994, which was enacted to provide the necessary legal modifications to increase the fight against the traffic and sale of drugs. This law is restricted to the provisions of article 29 of the Constitution. Thus, no recording of telephone conversations is permitted, because it would be in violation of the constitutional norm, and

  (iii) Law No 11 of January 22, 1998, which is the first example of legislation in connection with the regulation of information stored by electronic means.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Law No 81 created a self-regulatory body—the Personal Data Protection Council—to advise the existing government regulator, the National Authority for Transparency and Access to Information, on the enforcement and regulation of private data or personal data matters in Panama.

The National Authority for Transparency and Access to Information has created a special department authorized to receive complaints, investigate and sanction all individuals, companies or custodians responsible for processing personal data.

2 SCOPE

2.1 Which companies are subject to privacy law in Panama?

All companies in Panama are subject to privacy law, since privacy rights are guaranteed by the Political Constitution.

As far as personal data is concerned, any individual or legal entity, public or private, commercial or non-profit, that processes personal data will be subject to Law No 81, and must comply with the law to guarantee its rights and principles.

2.2 Does privacy law in Panama apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The personal data protection provisions of Law No 81 do not apply to companies outside of Panama, since the legislator did not include obligations for companies processing personal data outside of the country.

The provisions of Law No 81 will be applicable to foreign companies or companies owned by individuals that are not in Panama, if the processing of the personal data takes place in Panama.

The provisions of Law No 81 will be applicable to any individual responsible for collecting personal data if he is domiciled in Panama, or the database that contains the private data or personal data is in Panama.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Panama?

Law No 81 defines "personal data" as any information regarding an individual that may identify him/her or can make him/her identifiable.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

By Law No 81, "sensitive data" is "that which refers to the intimacy of its owner or that which, if wrongfully used, can lead to discrimination or entail a grave risk for its owner". The following personal data, among others, is considered sensitive:

(a) data that can reveal information such as racial or ethnic origin;

(b) religious, philosophical and moral convictions;

(c) union affiliations;

(d) political opinions;

(e) data concerning health, life or sexual orientation, genetic or biometrical data; and

(f) data subject to regulation and aimed at unequivocally identifying an individual.

In Panama, sensitive information or sensitive data may be transferred only in certain cases (see question 9.1).

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Under Law No 81, the key principles that must be followed in order to process personal data are the following:

(a) The Loyalty Principle: All the data that is collected and processed must be obtained without deceit or misrepresentation, and without using methods that are fraudulent, false or illicit.

(b) The Principle of Purpose Limitation: The personal data processed must be collected for the legitimate purposes specified when the data was collected. The private data or personal data may not be used later for another purpose incompatible or different to the purpose for which it was initially requested, or be kept for longer periods of time than initially authorized.

(c) The Proportionality Principle: Only data that is appropriate, pertinent and limited to the minimum necessary for the purpose for which it is collected, should be requested.

(d) The Veracity and Exactitude Principle: The personal data must be accurate and up-to-date in a manner that responds truthfully to the current situation of the owner.

(e) The Data Security Principle: Those responsible for processing personal data must take the necessary steps to implement such technical and organizational measures as are required to guarantee the security of the data under their care, particularly if such data can be considered sensitive data, and must inform the owner of the data, as soon as possible, whenever data has been extracted without authorization or there are indications that suggest a security breach has occurred.

(f) The Transparency Principle: All information and communications with the owner of the personal data concerning its treatment must be made using language that is simple and clear, and the owner must be kept informed at all times of his/her rights as owner of the data, and of the possibility of enforcing his/her rights to access, rectify, cancel, oppose or transport his/her personal data.

(g) The Confidentiality Principle: All those who have contact with the collected personal data must maintain the secret and confidential nature of the data, even after the relationship with the owner of the data, or the person or company responsible for collecting the data, has finished, preventing the access or unauthorized use of the private data or personal data.

(h) The Legality Principle: In order for the processing of personal data to be considered legal, the data must be obtained and processed either:

  (i) with previous, informed and unequivocal consent from the owner of the data; or

  (ii) supported by the law, ie:

    (1) that the processing of the personal data is necessary to execute a contractual obligation, provided that the owner of the data is a party to the contract.

    (2) that the processing of the personal data is necessary to complete a legal obligation, or

    (3) that the processing of personal data is expressly authorized by a special law.

(i) The Portability Principle: The owner of the data has the right to obtain from the person or company responsible for processing the data, a copy of his/her data structured in a generic and commonly used format.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Law No 81 establishes two possible roles for companies, based on how they process personal data:

(a) Database custodian: the individual or company that acts on behalf of an individual or company that is responsible for processing the data by safekeeping and preserving a database; and

(b) Data controller: the individual or company responsible for the decisions related to the processing of data and who determines the objectives, means and scope of such processing.

The individual or company responsible for the processing of personal data contained in a database will establish the protocols and procedures for its management and safe transfer, protecting the rights of the owners of the data. These duties will be monitored and supervised by the National Authority for Transparency and Access to Information.

The database custodian must take due care of the data, as he/she will be held jointly responsible for any damages or harm caused.

Law No 81 does not include provisions specifically aimed at regulating obligations and contractual requirements based on the roles of database custodian or data controller. The implementing regulations should deal with these matters.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Law No 81 contains certain provisions that broadly refer to issues such privacy policies, risk impact assessments and record keeping, including the ones listed below. It is worth noting that the implementing regulations should introduce provisions addressing these and other matters.

A "sector regulator" will determine the minimum requirements concerning the content of privacy policies, protocols, processes and procedures for processing and safe transfer of data.

When the collection of information is made via the internet or any other digital communication platform, the obligations established by the law will be complemented with the disclosure of privacy policies and/or terms applicable to the services available. If the consent of the owner is given in a written declaration that also refers to other matters, the consent must be presented in such a way that it is clearly distinguished from the rest, is comprehensible and easily accessible, using clear and simple language.

There is no specific reference in the Law to "risk impact assessments" but operators that manage public networks or render communication services available to the public must warrant the protection of personal data in accordance with the law and the regulations that implement it. They must also adopt proper management and technical measures to preserve the security in the use of the network or the rendering of services, with the aim of guaranteeing the level of personal data protection required by this law and its regulations, as well as the certifications, protocols, standards, and other measures established by the competent authorities.

Those responsible and/or custodians of databases that transfer personal data stored in databases to third parties must keep a record of such transfers, which must be made available to the regulator if required to comply with the law. For each of these databases, the records must include:

(a) their identification and that of whoever is responsible for them,

(b) the nature of the stored personal data,

(c) the legal ground for their existence,

(d) the procedures for the collection and treatment of data,

(e) the destination of the data and the individuals or entities to whom they can be transferred,

(f) the description of the group of individuals that it includes,

(g) the safety measures, the protocols and the technical description of the database,

(h) the way and conditions in which individuals can receive or access their data,

(i) the procedures required for the rectification and updating of data, and

(j) how long the data may be stored,

and any change in the aforementioned; in addition, the records must identify all those who have accessed the personal data within the previous fifteen days and state how long each person had access for.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Panama? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

In Panama, the individual or company that processes personal data is responsible for the integrity of the data and must protect it by setting up protocols, processes, administrative procedures and secure transfer of the data. Law No 81 provides general guidelines that should be more specifically addressed in the implementing regulations that are pending.

The minimum standards for securing data and rights of the owners of the personal data are overseen and supervised by the National Authority for Transparency and Access to Information, together with the National Authority for Governmental Innovation.

6.2 How are data breaches regulated in Panama? What are the requirements for responding to data breaches?

According to Law No 81, if a person or a company that processes or controls private data or personal data suffers a security breach of the data, it is obligated to inform the authorities and the owner of the data about the security breach. In cases where there is security breach in a public communication network, the operator that manages the network, or that provides the communication service, must inform the owner of the data about the security breach.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Law No 81 expressly indicates that all individuals shall have the following rights in connection to their personal data:

(a) the right to access their personal data and to know the origin and purpose for which they have been collected;

(b) the right to rectify their personal data;

(c) the right to cancel the use of their personal data;

(d) the right to oppose to the use of their personal data;

(e) the right to data portability; and

(f) the right not to be subject to a decision based only on the automatized processing of his/her personal data that produces negative legal effects or negatively affects his/her rights, when the decision has to assess certain aspects of personality, health, labour performance, credit, reliability, conduct, characteristics, among others, except when:

  (i) there is consent of the owner of the data,

  (ii) it is required to execute or comply with a contract or legal relationship between whoever is responsible for the processing of data and its owner, or

  (iii) when it is authorized by special laws or future regulations.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

In Panama, a person or company that markets or advertises its goods or services online via digital media or other types of digital marketing communications, using personal data, must comply with the requirements of Law No 81. In order to comply with the law, the individual or company must obtain prior consent of the owner of the personal data. To obtain legal consent, the request for the personal data must specify:

(a) the name and any additional information needed to clearly identify the individual or company requesting the personal data;

(b) the motive and the purpose for requiring the personal data;

(c) what personal data is subject to transfer; and

(d) the duration of time for which the individual or company is authorized to use the personal data.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Under the provisions of Law No 81, if a person or company uses tracking technologies to collect or process personal data, it will be subject to the general rules and principles that apply to the processing of personal data.

The individual or company that will use personal data with tracking technology must obtain unequivocal consent from the owner to the processing of the data and must inform the owner how the data will be used. Such consent must be obtained in a way that allows the traceability of the consent.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Under the provisions of Law No 81, personal data may only be used for the fixed, explicit and lawful purpose that the owner has authorized. In view of this, any person or company carrying out targeted advertisements and behavioral advertising using personal data must obtain prior consent.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Under Law No 81, advertisers that intend to share data with third parties must obtain unequivocal consent from the owner in order to use the personal data for customer matching.

Consent to use the personal data for customer matching must be obtained in a way that allows traceability of the consent.

8.5 Are there specific privacy rules governing data brokers?

Under Law No 81, data brokers are responsible for the protocols, processes and procedures necessary to protect the personal data under their care. Additionally, data brokers are required put in place protocols to safely transfer data.

All data brokers in Panama are supervised by the National Authority for Transparency and Access to Information with the support of the National Authority for Government Innovation.

Data brokers must implement the minimum requirements that must be contained in the privacy policies, protocols, processes and procedures for processing and providing a secure transfer of the personal data.

8.6 How is social media regulated from a privacy perspective?

In Panama, individuals or companies using social media networks or public media companies in order to provide services using personal data must obtain prior consent. All individuals or companies using personal data are subject to the provisions of Law No 81 and must guarantee the owner of the data that the data will be protected.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Law No 81 does not contain provisions concerning loyalty programs and promotions, but, from a privacy perspective, the individuals or companies providing these services are required to follow the general rules and regulations to legally process personal or private data; ie, all the standards, rules, certifications, protocols, technical processes and administrative measures to preserve the security and provide the minimum levels of protection of the data.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Under Law No 81, the transfer of personal data will require the following:

(a) Consent from the owner of the personal data;

(b) The country to which the personal data is going to be transferred must have in place at least the minimum requirements set forth by Panamanian law;

(c) Sensitive data cannot be transferred unless:

  (i) the owner has provided consent, except when the law does not require it;

  (ii) when it is necessary to preserve the life of the owner of the sensitive data and he/she is physically and mentally incapable. In these cases, the guardian, executor or those who have the tutelage must give the authorization for the transfer of the sensitive data or sensitive information;

  (iii) When the data is necessary to recognize, exercise or defend a right in legal proceedings and there is authorization from the competent court; or

  (iv) When the objective is historical, statistical or scientific in nature. In these cases, the appropriate measures must be adopted to conceal the identity of the owner.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

According to Law No 81, when the transfer of the personal data is within the same economic group of companies, the data must be used for the same purpose.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Law No 81 authorizes the National Authority for Transparency and Access to Information to set monetary sanctions that may range between US $ 1,000 and USD$ 10,000.

Depending on the severity of the violation, the National Authority for Transparency and Access to Information may sanction infringers with a written warning, a citation before National Authority for Transparency and Access to Information, a fine, the closure of the database registration, or suspension and disqualification from processing personal data.

The law also categorizes violations into:

(a) minor infractions or violations;

(b) serious infractions or violations; and

(c) very serious infractions or violations.

10.2 Do individuals have a private right of action? What are the potential remedies?

Article 37 of Law No 81 specifies that the individual or company responsible for unlawfully processing of personal data is required to compensate the owner of the data for the monetary and/or moral damages caused.

A court of justice will prosecute actions filed against an individual or company for unlawful processing personal data.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Panama which affect privacy?

There are no rules particular to the culture of Panama that will affect privacy. In any case, it is the lack of regulation that may influence how privacy is dealt with. Adopting a personal data protection law is a big step forward, as it sets new standards and principles to guarantee the protection of confidential, sensitive and personal data.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Law No 81 has been recently enacted. It will become effective in 2021. In the meantime, the government has to approve the implementing regulations, which will surely enter into more details than the law. Significant developments are therefore expected in the next two years.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Panama?

Since Law No 81 has been recently enacted and will become effective in 2021, all those who are involved in the processing personal data should carefully review it to confirm that they are in compliance before March 26, 2021.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The privacy landscape in Panama has evolved significantly in the past few years. Until recently, privacy matters were only regulated by several different legal provisions scattered between national laws and the Constitution. Since the enactment of Law No 81, the privacy landscape now has a specific law concerning personal data protection. Hopefully, this will bring more attention to privacy law in general, and will help to organize and regulate it properly.

12.2 What do you envision the privacy landscape will look like in 5 years?

With the newly enacted Law No 81 of March 29, 2019 becoming effective in 2021, in five years from now Panama will have data protection standards similar to those that have been in place for many years in other countries. Local individuals and companies currently processing personal data will have adopted the rules set out in Law No 81, and consumers will be aware of their rights. National authorities will have further developed the principles and regulations contained in this law, and specific aspects concerning advertising and privacy law will be dealt with in new laws.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Since the processing of personal data has only been recently regulated in Panama with the enactment of Law No 81, individuals and companies face the challenges that arise from making changes necessary to comply with the new regulations before the law becomes effective in 2021. Taking into consideration that this law introduces principles, rights, obligations and procedures that Panamanian consumers, individuals or companies are not familiar with, it is important for all parties to be sufficiently informed and be prepared by March 29, 2021 to comply with the provisions of Law No 81 and its implementing regulations.

PARAGUAY

1 PRIVACY LAW

1.1 How is privacy regulated in Paraguay?

In Paraguay, privacy law is regulated by means of several pieces of legislation, beginning with Paraguay's Constitution, which, in Article 33, 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, provided that this does not affect the public order established by the law, or third parties' rights, is exempted from the 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, which shall be referred to and explained below.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) National Constitution (see question 1.1);

(b) Criminal Code, which 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 his/her 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.

(c) 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.

(d) The Civil Code regulates rights associated with a person's name and establishes that anyone injured by means of the unlawful use of its name has a right of action to stop such unlawful use and to demand damages.

(e) Copyright law provides that the portrait of a person 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.

(f) Trademark Law protects people against the registration of their name.

(g) Law No 1682/01 "Which Regulates Information considered Private" ("Data Protection Law") establishes that:

  (i) any person has the right to collect, store and process personal data for strictly private use;

  (ii) public sources of information (eg, information with respect to a person's identity card number) are accessible to everyone and that every person has the right to access data that is registered before the Public Registry;

(iii) the collection, storage, processing and publication of data or personal characteristics for scientific and statistical purposes is legal, provided that the persons are not individualized.

(h) Moreover, the Data Protection Law stipulates that publicity or broadcasting of sensitive data related to persons that are expressly individualized or may be individualized is prohibited. The Law considers that "sensitive data" is information regarding race or ethnical origin, political preferences, an individual's state of health, religious or philosophical conviction, amongst others.

(i) Data regarding individuals or corporations that reveal their financial situation or solvency shall be made available under certain conditions;

(j) Law No 4868/12 "On Electronic Trade" provides 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.

(k) The Law on Protection of Consumers, which regulates advertisement, 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 Law on Consumer Protection.

(l) Finally, the terms of the Advertising Self Regulation Code, enforced by the Center of Regulations, Norms and Communication Studies, stipulate that "all advertising will be carried out with a sense of social responsibility ... characterized by respect for the dignity of the human person, their privacy, the family nucleus.... All advertising activity must adhere to morality, good customs and public order."

By which, *contrario census,* the unlawful publication or broadcasting of an individual's private data/information would be a violation to the terms of such Self Regulation Code.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Privacy law is 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 that, as a result of an illegitimate act or omission, whether coming from an authority or an individual/corporation, considers himself/herself 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 such 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.

2 SCOPE

2.1 Which companies are subject to privacy law in Paraguay?

All companies within the Paraguayan jurisdiction are subject to privacy law.

2.2 Does privacy law in Paraguay apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 INFORMATION

3.1 How is personal information/personal data defined in Paraguay?

There is more than one definition of "private" or "personal" information/data in Paraguay.

The Paraguayan Criminal Code defines "intimacy" (private data) as the intimate personal sphere of a person's life, specially related to his/her family, sexual life and state of health.

The Data Protection Law does not give a precise, exact definition of what is to be understood by "private information", but its definition can be deduced from several articles to mean sensitive data regarding explicitly individualized persons (or persons who may be individualized), related to their political preferences, state of health, religious convictions, sexual intimacy and economical or financial status, amongst other matters.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

All information that refers to a person's intimacy may be considered "sensitive data", eg: a person's state of health, his/her sexual preferences, his/her religious convictions, his/her political preferences. 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 work telephone number). Sensitive data may even refer to a person's financial status.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Above all, respect. A company should also be transparent as far as personal data information is concerned and should use the information in a limited way.

In this sense, the Data Protection Law provides that, where companies that store, process and publicize information regarding a person's financial status, or his/her compliance with his/her economical/commercial obligations, the following is applicable:

(a) Some information regarding a person's financial status may be publicized, but such information needs to be constantly updated, as well as the person's fulfilment or compliance with his/her commercial obligations; such updating of information should be done within two working days from the date the data is made accessible to the company, directly or by means of the party affected.

(b) Such companies cannot provide information regarding debts that:

(i) have become overdue but have not been legally claimed, where the debt is no more than 90 days overdue;

(ii) that have not been legally claimed, where four years have passed since their registration and there are no new non-compliances or debts incurred into by the same debtor; or

(iii) have been claimed in a judicial trial, where the prosecution has lapsed,

among other circumstances.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

According to the Law on Consumer Protection, providers of goods and/or services must provide consumers with their name and address. In addition, the Law on Electronic Trade provides that providers of goods and services by electronic means or remotely must provide, or make accessible to consumers, their corporate name, address, name of the company's owners, email address and telephone number.

As for privacy policies, the Law on Electronic Trade establishes that providers of goods and services by means of the internet or remotely must inform consumers/users as to their privacy policy regarding the use of their personal data.

Providers of internet or electronic intermediation services and providers of data hosting services must keep records of the connection and traffic data generated by means of the communications established during the provision of a service for a period of at least six months. The data to be stored is solely for the identification of the origin of the hosted data. Companies may not use the data collected for purposes other than those established by Law, and must adopt sufficient security measures to avoid the loss or alteration and non-authorized access to the data.

There is no specific requirement to register with a privacy authority, nor to conduct a risk impact assessment.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Paraguay? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

There are no specific standards regarding data security in Paraguay.

However, 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.

Privacy and data security are also protected at a Constitutional level.

6.2 How are data breaches regulated in Paraguay? What are the requirements for responding to data breaches?

(a) Under the National Constitution, documentation pertaining to a person, as well as his/her data, is secured. By the writ of *Habeas Data,* all persons may access the information and data about themselves, or about their assets, that is held in official or private registries of a public character, as well as to know the use make of the same, and of their end. They may request the competent courts to update, rectify or destroy any such data which may be erroneous or illegitimately affects his/her rights.

(b) The Criminal Code punishes felonies such as that imply the "listening, storage and revealing to third parties of private communication pertaining to a particular person, as well as the revealing of secrets that have a 'private character'", among others.

(c) Corporations in general (especially under the terms of the Law on Electronic Trade) cannot reveal a person's personal information or data.

The means to respond to such breaches include the filing of criminal complaints (if a felony has been committed) or lawsuits before the civil courts.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

All those mentioned above: personal information and or/data is not accessible to third parties, unless required by a competent judge.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Most marketing communications are not regulated from a privacy perspective.

However, Law No 5830/17 "Which Prohibits Non-Authorized Publicity for Mobile Phone Users/Holders" has recently established a National Registry within the National Office of Consumer and User Protection ("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 the Law.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The use of cookies, pixels, etc, is not specifically addressed by the Paraguayan legislation.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The use of targeted advertising and behavioral advertising is not specifically addressed by the Paraguayan legislation.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Currently, there are no notices and/or consents that advertisers need in order to share information regarding consumers with third parties for customer matching; however, under the Data Protection Law, certain data regarding consumers should not be shared with third parties within companies.

8.5 Are there specific privacy rules governing data brokers?

There are no specific privacy law governing data brokers.

8.6 How is social media regulated from a privacy perspective?

Social media is not yet regulated in Paraguay.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs are not specifically addressed by the Paraguayan legislation. As far as promotions are concerned, the only types of promotions regulated are those concerning games of chance, which must be registered before the National Commission of Games of Chance ("Conajzar"), subject to payment (as a fee) of a percentage of the amount of the prize to be granted to the winner.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

No, except for the general landscape governing the use of a person's private/intimate/personal information.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

None other than those mentioned above.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 individuals have a private right of action? What are the potential remedies?

Yes. Individuals may file complaints before the civil and the criminal courts.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Paraguay which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Not at the moment.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Paraguay?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

During the past few years, a major regulation, the Law on Electronic Trade, has been issued, which provides several obligations on companies whose main activities concern the provision of services by electronic means (whether by provision of goods by an internet website, the hosting of a website, etc). In our understanding, those changes were propelled by the world's current situation, by global trends, and by the introduction into Paraguay of modern technology, especially the digital signature and the electronic signature.

Also, a "do-not-call" registry has been set up with the objective of forbidding companies to contact consumers on mobile phones where consumers have registered with the Registry for the specific purpose of not being contacted (see question 8.1).

Those two regulations are great advances for Paraguay with respect to the protection of consumers.

12.2 What do you envision the privacy landscape will look like in 5 years?

In our opinion, Paraguay will have to ensure its legislation is adequate to meet worldwide trends: data protection, social media regulation and further regulation with respect to advertising.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The challenge companies may face is regarding respect for people's personal data. Such respect may not affect companies for the moment, but it will become a major issue in years to come, especially when dealing with companies with strict data protection regulations. And in that respect, it is important that companies undertake action, campaigns, risk assessments, etc, in order to be prepared for compliance with this and any new legislation which may be passed.

PERU

1 PRIVACY LAW

1.1 How is privacy regulated in Peru?

Data privacy rights are regulated by law (see question 1.2).

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) Law No 29,733 on Personal Data Protection;

(b) Supreme Decree No 003-2013-JUS, which approves the Regulations under Law on Personal Data Protection.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Data privacy law is enforced by the General Direction of Data Privacy Protection of the Ministry of Justice ("Data Privacy Authority").

2 SCOPE

2.1 Which companies are subject to privacy law in Peru?

The Law on Personal Data Protection applies to both the public and private sectors that treat data and protects all personal data of natural persons.

2.2 Does privacy law in Peru apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

No. Peruvian law applies only to Peruvian companies, private or public, that treat data from individuals.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Peru?

"Personal data" is defined by the Law on Personal Data Protection as all information about a natural person that identifies or makes him/her identifiable through means that can be reasonably used.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" is defined by the Law on Personal Data Protection as biometric personal data that by itself can identify the holder; and data relating to:

(a) race and ethnicity;

(b) political, religious, philosophic or moral convictions or opinions;

(c) economic income;

(d) trade-union membership;

(e) health or sexual life; or

any similar information that might affect a person's privacy.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, and purpose limitation)?

Personal data must be treated with full respect of the fundamental rights of the data subject and the rights conferred by the Law. The same rule applies for its use by third parties. Personal databank controllers and personal databank processors must comply with the eight Guiding Principles:

(a) legality,

(b) consent,

(c) purpose,

(d) proportionality,

(e) data quality,

(f) security,

(g) recourse, and

(h) adequate protection,

according to the Law.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No. The obligations and contractual requirements on database owners and processors are the same for all companies.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Databanks must:

(a) register their banks before the Data Privacy Authority;

(b) communicate the cross-border data transfer flow to the Data Privacy Authority;

(c) have an adequate level of security to protect from breaches;

(d) use the data only for what they have inform the data subject;

(e) obtain consent from the data subject to treat their data; and

(f) post their terms and conditions and privacy policies on their websites so data subjects are aware of them.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Peru? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Data security is regulated by the Law on Personal Data Protection. Personal databank controllers must adopt technical, organizational and legal measures to guarantee the security of personal data and avoid alteration, loss, treatment or unauthorized access to it. The security requirements and conditions to be met by personal databanks are established by the National Data Protection Authority, unless prescribed by special rules contained in other laws.

Processing of data in personal databanks that do not meet these requirements is prohibited.

6.2 How are data breaches regulated in Peru? What are the requirements for responding to data breaches?

It is regulated by law. There is no obligation to notify a breach to the Peruvian Data Privacy Authority; however, it is recommended to notify affected individuals in order to avoid them complaining to the Data Privacy Authority. Database holders and data handlers must adopt technical, organizational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Data subjects have the "ARCO" rights with respect to their personal information/personal data. These are the rights of:

(a) Access;

(b) Rectification;

(c) Cancellation; and

(d) Opposition.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

This kind of communications is 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, in order for the data subject to identify it immediately and be aware of its content.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is no specific law regulating tracking technologies; however, taking into consideration the Law on Personal Data Protection, the data subject must grant its consent to be tracked by the different online technologies, eg, cookies.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertising and behavioral advertising are not specifically regulated in the Law on Personal Data Protection, nor the Advertisement Law. General law will apply, depending on the case.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

In order to share data with third parties, advertisers need to inform the data subject and receive an express consent.

8.5 Are there specific privacy rules governing data brokers?

There are no specific privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

There are no specific privacy rules governing social media, but the Law on Personal Data Protection can apply to privacy matters related to social media, among other laws regarding the matter.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are no specific privacy rules governing loyalty programs and promotions. However, the general Law on Personal Data Protection can apply to privacy matters related with loyalty programs and promotions. In practice, companies operating these kinds of programs and promotions must obtain consent from the data subject in order to use his/her personal information and to send emails and notices and to use its consumer habits. Such consent is mandatory.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The personal databank controller and the personal databank processor may transfer personal data cross border only if the destination country maintains an adequate level of protection according to the Law on Personal Data Protection. In the case that 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 Law on Personal Data Protection.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

No. However, there are exemptions from the general rule, and guarantees (see question 9.1) are not required in the following situations:

(a) agreements within the framework of international treaties to which Peru is a party;

(b) international judicial cooperation;

(c) international cooperation among intelligence agencies for the fight against terrorism, illicit drug traffic, money laundering, corruption and trafficking of persons and other forms of organized criminal activity;

(d) 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;

(e) when related to bank or stock market transfers, in relation to the respective transactions and according to the applicable law;

(f) when the cross-border flow of personal data is performed for the protection, prevention, diagnosis or medical or surgical treatment of its holder, or when it is necessary for the performance of epidemiological or similar studies, as long as adequate dissociation procedures are applied; and

(g) when the data subject has given his/her previous, informed, express and unequivocal consent.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Violations of privacy or data security law are punishable by administrative civil penalties, namely fines ranging from 0.5 UIT to 100 UIT (approx US $ 650–US $ 130,000).

10.2 Do individuals have a private right of action? What are the potential remedies?

Under the Law on Personal Data Protection, an individual can request a company to correct/delete their data.

Individuals can file a civil action in the courts requesting damages for breach of privacy.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Peru which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

There is only one data protection Law and its Regulations. The Peruvian Law on Personal Data Protection was enacted in July 2011 and entered into force in May 2015, so it is a relatively new Law.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Peru?

Our main advice to clients is to always:

(a) obtain consent from the data subject; and

(b) inform the data subject why is his/her data been collected and the intended final use of it.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

As mentioned, the Law is quite new, so there have not been too many changes in the privacy landscape.

12.2 What do you envision the privacy landscape will look like in 5 years?

Hopefully, privacy will be taken much more seriously, because, at this moment in Peru, people and companies lack knowledge about privacy rights.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

As mentioned before, many Peruvian companies lack knowledge regarding privacy rights and have committed breaches because of this. For example, companies may not know that they need to register their databanks before the Data Privacy Authority (see question 5.1).

Therefore, it is important that the government inform the people about privacy rights and obligations.

PUERTO RICO

1 PRIVACY LAW

1.1 How is privacy regulated in Puerto Rico?

Puerto Rico currently has two laws related to privacy and a pending bill. This legislation is directed at compulsory notifications regarding security breaches and privacy policies.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Key laws regulating privacy are:

(a) Citizens' Information about Database Security Act (Act No 111-2005); and

(b) Privacy Policy Notification Act (Act No 39-2012).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Individuals may file actions for civil damages based on the aforementioned laws or the Civil Code Article 1802.

2 SCOPE

2.1 Which companies are subject to privacy law in Puerto Rico?

Any company that keeps a database containing customer personal information is subject to privacy law in Puerto Rico.

2.2 Does privacy law in Puerto Rico apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Current legislation applies to any company that keeps personal data of Puerto Rico users.

There are no specific obligations for companies outside the country.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Puerto Rico?

"Personal information" is "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."

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Personal information that is considered sensitive includes: 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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Notice to users.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Give notice to users regarding the privacy policy and any security breaches that may compromise personal data.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Puerto Rico? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

There is no regulation except for notice of breach.

6.2 How are data breaches regulated in Puerto Rico? What are the requirements for responding to data breaches?

Breaches must be informed to users. Users may file a damages action if harmed by a breach.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

N/A

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

N/A

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

N/A

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

N/A

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Privacy policy must include the third party with whim the data is shared.

8.5 Are there specific privacy rules governing data brokers?

N/A

8.6 How is social media regulated from a privacy perspective?

N/A

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

N/A

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

N/A

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

N/A

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

A fine of up to $5,000.

10.2 Do individuals have a private right of action? What are the potential remedies?

Actions for damages may be filed. Injunctions and monetary relief may be obtained.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Puerto Rico which affect privacy?

N/A

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Senate bill 1231, related to the protection of online privacy, is pending approval.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Puerto Rico?

Puerto Rico is a US territory, which means any federal law regarding personal data and privacy is applicable.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Legislators are more aware of privacy issues due to the increased use and reliance on social media.

12.2 What do you envision the privacy landscape will look like in 5 years?

We do not envision many changes.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Obtaining and maintaining user trust regarding the use and protection of their data.

RUSSIA

1 PRIVACY LAW

1.1 How is privacy regulated in Russia?

Under Russian laws, individuals enjoy the right to privacy, which, in particular, includes protection of their personal data. Russian data privacy regulations are based on the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), Articles 23 and 24 of the Russian Constitution, several federal laws and administrative regulations.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Key Russian laws and regulations include the following:

(a) Federal Law dated July 27, 2006 No 152-FZ "On Personal Data" ("Personal Data Law") that is the principal law in the area of personal data protection, which contains certain specific provisions governing processing of personal data for direct marketing purposes;

(b) Federal Law dated July 27, 2006 No 149-FZ "On Information, Information Technologies and Protection of Information" that sets out certain general principles regarding protection of information, as well as a number of specific rules governing use of information technologies;

(c) Federal Law dated March 13, 2006 No 38-FZ "On Advertising", which is the principal law in the area of advertising and contains some provisions on distribution of advertising materials via communication channels;

(d) Federal Law dated July 7, 2003 No 126-FZ "On Communications", which governs the provision of communications services in the Russian Federation and, among other elements, sets out the rules relating to mailings carried out by communication providers through communication channels, either for themselves or on behalf of their partners (contractors); and

(e) Labor Code of the Russian Federation dated December 30, 2001 No 197-FZ, which sets out a number of specific requirements relating to the processing of employees' personal data.

In addition to the above, Russian state authorities have issued a number of regulations and guidelines governing various aspects of personal data processing and protection, such as the processing of personal data without automated means, security requirements, etc. The key by-laws are:

(f) "Requirements to Security of Personal Data Processed in Information Systems of Personal Data" approved by the Decree of the Government of the Russian Federation dated November 1, 2012 No 1119;

(g) "Scope and Composition of Organizational and Technical Measures to Ensure Security of Personal Data Processed in Information Systems of Personal Data" approved by the Order of the Federal Service for Export and Technical Control dated February 18, 2013 No 21; and

(h) "Scope and Composition of Organizational and Technical Measures to Ensure Security of Personal Data Processed in Information Systems of Personal Data with Use of Cryptographic Protection of Information Required to Comply with Personal Data Security Requirements Stated by the Government of the Russian Federation with respect to each Security Level" approved by the Order of the Federal Security Service dated July 10, 2014 No 378.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The main regulators in the area of data protection are:

(a) Federal Service for Supervision of Communications, Information Technology, and Mass Media ("Roskomnadzor") is the supervisory authority in the area of personal data protection (ie, the data protection authority). It carries out its functions through its central and regional offices, which are responsible for supervising data controllers in their respective regions of Russia;

(b) Russian Federal Antimonopoly Service ("FAS") is the supervisory authority in the area of competition and advertising;

(c) Russian Federal Service for Technical and Export Control ("FSTEC") is the authority responsible for supervising the protection of confidential information with use of technical tools; and

(d) Russian Federal Security Service ("FSB") is the authority responsible for supervising the protection of confidential information with use of encryption tools.

Supervisory activities in the area of personal data protection are performed by Roskomnadzor by way of scheduled inspections, unscheduled (ad hoc) inspections and the monitoring of data protection activities through the Internet without interaction with a company whose data processing activities are being monitored. Roskomnadzor may cooperate with the FSTEC and FSB in the course of its supervisory activities. As for the FAS' supervisory activities in the area of advertising, they include unscheduled inspections and monitoring.

2 SCOPE

2.1 Which companies are subject to privacy law in Russia?

Privacy law applies to any entities, including state and municipal authorities, legal entities and individuals that carry out processing of personal data by automated means, or without automated means if such manual processing is similar to automated processing, ie, it enables algorithm-based search of personal data contained in card catalogues or repositories.

Privacy laws apply to entities having physical presence in Russia and processing personal data there, and also those without a physical presence in Russia, but processing personal data through the websites and apps which target a Russian audience. The "targeting" test is quite broad and involves an examination of diverse factors, such as the use of the Russian language on the website, registration of a domain name in the Russian domain zone, the possibility of choosing Russia as a place for delivery of products, registration of users from Russia (indicating Russia as a territory), etc. Targeting criteria are not formalized under the Russian laws so that they are defined on-a-case-by-case basis.

2.2 Does privacy law in Russia apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Russian privacy law applies to companies outside the country and to those which do not have physical presence in Russia (eg, no branch or representative office). The targeting of a Russian audience through a website or app where personal data is processed serves as a criterion as to whether Russian laws apply (see question 2.1). Russian laws do not set out any specific obligations for foreign companies, so that the general requirements apply.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Russia?

"Personal data" is defined as any information relating to an identified or identifiable, directly or indirectly, individual (data subject). This definition is based on Convention 108 and quite similar to the one laid down under the EU data protection laws.

In practice, the notion of personal data is construed broadly so that, along with information traditionally attributed to personal data (such as name, contact details, etc), it may also include certain technical (eg, information processed with use of cookies) and other data.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

By the Russian Personal Data Law, "sensitive personal data" is defined as personal data relating to race, national origin, political views, religious and philosophical commitments, intimate life and health. In addition, sensitive data includes data relating to criminal convictions.

As a basic rule, sensitive personal data (except data relating to criminal convictions) may be processed only on the basis of an individual's written consent, executed in hard copy or as a digital document signed by reinforced digital signature (a type of digital signature based on state-certified cryptographic algorithms). In addition, such consent must contain certain mandatory elements prescribed by law. Exceptions exist where consent is not required; however, they are very limited and apply rarely.

There is a general prohibition on the processing of data relating to criminal convictions. Exceptions are very limited and apply very rarely.

Additionally, Russian privacy law distinguishes a separate category of privacy-sensitive information — "biometric personal data" — which is defined as information relating to an individual's physiological and biological characteristics, enabling and used for the individual's identification (eg, fingerprints, personal image, voice recording, etc). In addition, there is a draft law aimed at extending the scope of biometric data in the context of modernizing Convention 108. If adopted, biometric data will include genetic information.

As for the processing of sensitive data, biometric data processing may be performed only on the basis of the individual's written consent, unless certain exceptions apply.

Apart from the above, in terms of security, the Russian data protection laws imply that the scope of security measures to be implemented by the controller depends on relevant security threats, the number and categories of data subjects, and the types of personal data being processed — where information systems contain biometric or sensitive data, higher security standards apply.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The key privacy principles relating to the processing of personal data are set out by the Personal Data Law, and are:

(a) Lawfulness: the processing of personal data must be lawful. In particular, this principle implies the need to ensure that there are legal grounds for data processing by the data controller.

(b) Purpose limitation: implying that processing of personal data must be limited to the achievement of a specific lawful purpose, and personal data must not be processed for other, incompatible, purposes.

(c) It is prohibited to accumulate databases containing personal data processed for different, incompatible, purposes.

(d) Data minimization: implying that the scope and content of personal data must be limited to what is necessary to achieve the specific data processing purpose. Personal data being collected and processed must not be excessive for the declared processing purpose.

(e) Personal data must be kept accurate, complete and up to date. The data controller must rectify or delete data which is inaccurate or incomplete.

(f) Once the processing purposes have been achieved, personal data must not be stored in a way allowing identification of the data subject (ie, it must be destroyed or anonymized), unless otherwise provided by legislation or agreement in which the data subject is a party, beneficiary or guarantor. Once the purposes of processing are achieved, personal data must be destroyed or anonymized, unless otherwise is provided by legislation.

(g) Personal data must be kept secure and confidential. The data controller must ensure the implementation of legal, technical and organizational measures to prevent unauthorized or uncontrolled access, modification, destruction or other unlawful operations on personal data.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The Russian Personal Data Law defines two roles in terms of data processing:

(a) Data controller: An entity arranging and/or carrying out processing of personal data, as well as defining the personal data processing purposes, the scope of personal data to be processed and personal data processing operations; and

(b) An entity processing personal data upon a data controller's assignment/instruction, which is similar to the notion of data processor under EU laws. To formalize an entity as a data processor, the controller and the entity must execute a data processing agreement (assignment) specifying:

(i) the processing purpose,

(ii) the data processing methods and operations performed by the processor,

(iii) the processor's security and confidentiality obligation, and

(iv) a set of security measures implemented by the processor.

The laws do not provide for any detailed guidance on a data processor's role and obligations. The Russian laws imply that the data processor is not responsible for requesting the individual's consent, which must be done by the controller. The controller will be responsible to individuals for the processing of their personal data by a processor under the controller's instructions.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Key obligations required by privacy law related to advertising activities are as follows:

(a) Legal grounds for personal data processing: There must be a legal ground for processing personal data (eg, consent, contractual necessity, legitimate interest, etc). The Russian authorities are quite conservative in this regard, so, in practice, consent is the most widespread legal ground. Moreover, in some cases, the law defines an individual's consent as being the only appropriate legal ground. For example, any direct marketing communications to an individual require the individual's explicit (opt-in) consent. The laws do not set out any legal exceptions (such as controller's legitimate interest) to this.

(b) Privacy Policy: A data controller must draw up a privacy policy and make it available to individuals concerned, in Russian, by publishing it on its website. The privacy policy must outline all aspects of the data processing performed in a transparent manner.

The Russian Personal Data Law sets out the information regarding personal data processing that must be communicated to an individual prior to personal data processing, which must be taken into account when drafting a privacy policy. In addition, Roskomnadzor has issued its recommendations on the content of privacy policies. Although these recommendations are not legally binding, they demonstrate the aspects of privacy which are taken into account by the regulator in this regard.

In light of the above requirement and recommendations, a privacy policy must contain the following details:

(i) data controller's identity (name, address);

(ii) terms and definitions used in the document;

(iii) explanation of the policy's goals;

(iv) purposes of data processing;

(v) legal grounds for data processing, categories of data subjects whose personal data is processed, and categories of personal data being processed;

(vi) types of processing operations to be performed and a general description of personal data processing methods;

(vii) information on transfer of personal data to the third parties, including cross-border transfer of personal data;

(viii) information on the data processors engaged to process personal data on behalf of the data controller;

(ix) information on measures taken to ensure the security and confidentiality of personal data;

(x) terms of personal data processing, including retention terms and conditions regarding termination of processing; and

(xi) data subjects' rights and how they can be exercised.

(c) Direct marketing requirements: Direct marketing communications with data subjects are subject to their prior opt-in consent (there are no exceptions in this regard).

Each marketing communication must contain either a link allowing data subjects to unsubscribe from further receipt of such marketing communications or, alternatively, information on how the recipient can unsubscribe. Once a data subject withdraws his consent to marketing communications, the data controller must immediately terminate direct marketing communications and the processing of personal data for this purpose.

(d) Localization of Russian citizens' personal data: Data controllers must ensure that certain operations with Russian citizens' personal data are performed in a database located in Russia. Such operations include recording, systematization, accumulation, storage, specification (update, modification), and retrieval. Afterwards, personal data can be transferred outside Russia, subject to cross-border data transfer requirements.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Russia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The basic obligation of a data controller is to ensure the security and confidentiality of processed personal data, which includes implementation of legal, administrative and technical security measures. Russian law sets out a very broad list of security measures that may be applied by a data controller (eg, appointment of a data protection officer, data recovery, implementation of internal policies, etc).

In addition to the general measures prescribed by law, the Russian Government has defined a number of specific measures a data controller must implement. The extent of these measures will depend on the types of security threat to the personal data, the number and categories of individuals whose personal data is processed, and the types of their personal data. Companies must perform security threat modelling in order to identify and categorize security threats that are likely to affect a database or system containing personal data. Based on security threat modelling, a company must determine the appropriate level of data protection and the particular set of security measures that must be implemented in order to safeguard the personal data.

6.2 How are data breaches regulated in Russia? What are the requirements for responding to data breaches?

Among other security measures, the security regulations require that the controller implements a number of security incident detection and response measures, eg, that it defines individuals responsible for incident detection and response, guides users to notify such individuals of security incidents revealed, etc. The extent of such measures will be defined by the controller based on threat modelling results (see question 6.1).

As for data breach notifications, the Personal Data Law does not currently require data controllers to notify either the regulator or individuals concerned when a data breach is revealed. There are certain industry-specific data breach notification obligations, eg, in the area of payment systems, critical information infrastructure, etc.

Meanwhile, in October 2018, Russia signed a Protocol amending Convention 108. When this Protocol comes into force, Russia will have to ensure that Russian laws set out the data breach notification procedure. In the light of this, Roskomnadzor officials have announced that they have already begun preparation of a draft bill to amend the Personal Data Law accordingly.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Russian privacy law sets out the following rights for individuals with respect to their personal data:

(a) To withdraw their consent at any time: In such case, the data controller should terminate personal data processing based on consent within 30 calendar days, unless other timeframes are agreed with the individual concerned or are set out in law. For example, the laws require that the data controller terminates direct marketing activities though communication channels and processing of personal data for such purposes immediately once the consent is withdrawn.

(b) To access personal data: A data subject is entitled to request from the data controller the confirmation that his personal data is being processed by that data controller and a range of details regarding such data processing activities (eg, categories of processed data, purposes of processing, operations performed on data, methods of processing, information on international transfers, etc). Upon the data subject's request, he should be provided with a copy of his personal data (eg, a copy of documents containing personal data, and extracts from automated information system where data is processed).

(c) To require correction of personal data which is incomplete, inaccurate, outdated or misleading: Upon receipt of a data subject's request, the controller must ensure that there is no further processing or use of such personal data until it has been corrected.

(d) To require that the data controller terminates the processing of his personal data and destroys personal data which is processed unlawfully or is not needed to fulfil the declared processing purpose (ie, is excessive): Personal data specified in the request will be blocked by the data controller while the circumstances subject to such request are investigated.

(e) Not to be subject to solely automated decision-making in the absence of a written consent: In addition, the data controller must explain to the individual the decision-making procedure, its implications, the individual's rights and how they can be exercised, as well as enable such individual to object to decisions made.

(f) To lodge a complaint against a data controller with a supervisory authority or a court.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Under Russian law, direct marketing communications with an individual are only permitted where the individual has provided a prior opt-in consent to receipt of marketing communications and processing of personal data for such purpose. No exceptions apply.

From a practical perspective, such consent may be obtained by use of a tick-box (digital or hard copy), or a "Subscribe" button, provided that such tick-box or button are separate from other consents (eg, acceptance of Terms of Use or processing of personal data as described in the Privacy Policy) and the tick-box is not pre-ticked. Otherwise, Russian regulators may not construe such consent as a valid legal ground and the data controller will be in breach of Russian data protection and advertising laws.

Each marketing communication must contain a link to unsubscribe from further receipt of such marketing communications or, alternatively, information on how the recipient can unsubscribe.

Once the data subject unsubscribes (withdraws its consent) from marketing communications, the data controller must terminate direct marketing communications and the processing of personal data for this purpose immediately — Russian laws do not provide any grace period in this regard.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Russian data protection laws do not directly address the issues of use of tracking technologies.

In general, Roskomnadzor and the courts consider such activities as personal data processing. An appropriate legal ground in such case will be the individual's explicit opt-in consent (eg, by tick-box form, banner, or pop-up window requesting the individual's consent on the home page of the website).

Use of purely technical cookies (ie, ones which are strictly necessary for the functioning of the website, unlike those allowing targeted advertisements, marketing analytics, etc) is a non-regulated area, and no unified approach exists as regards legal grounds for their use. Some companies stick to a risk-oriented approach, considering that consent is not required, and it is possible to rely on other legal grounds (such as preserving the legitimate interest of the data controller or contractual necessity). Others take a more conservative approach.

It is necessary to describe the use of tracking technologies and the corresponding data processing operations in the data controller's privacy policy or in a separate policy, eg, cookie policy. This policy must be available in Russian, and include the data controller' identity, explain what cookies and other technologies used are, their types, retention periods and the purposes for which they are used.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

In Russia, targeted advertising and behavioral advertising are not directly regulated from a privacy perspective. Since they imply collection and further processing of individuals' personal data, including use of cookies and other tracking technologies, the general rules apply. This means, in particular, that a data controller must ensure that there are appropriate legal grounds for such data processing and must inform the data subject how his personal data may be processed in the respective policy (eg, the privacy policy).

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The data controller must obtain the user's opt-in consent and set out details of the processing in its privacy policy in such a way that the data subject can get information on how his/her data will be processed.

8.5 Are there specific privacy rules governing data brokers?

There are no special regulations in Russian legislation regarding data brokers' activity. However, under the general rules, all data processing activities, including those of data brokers, must be carried out in compliance with the general requirements of the data protection laws.

8.6 How is social media regulated from a privacy perspective?

Processing of personal data in social media is based on the general rules and regulations and privacy principles. Terms of processing shall be described in the privacy policy, which must be available and transparent for data subjects (users of social media) and there must be an appropriate legal ground for such processing (such as consent, contractual necessity, etc.)

Additionally, when it comes to collection of personal data from social media, Roskomnadzor considers that this cannot be done freely by any third parties without sufficient justification to do so. Roskomnadzor's position (upheld in court practice) implies that users make their personal data available in social media profiles for specific purposes laid down by such social media Terms & Conditions and Privacy Policies. So, the purpose limitation principle applies and entities collecting individuals' personal data from social media must ensure appropriate legal grounds.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Russian privacy laws do not directly regulate loyalty programs and promotions. General rules apply to loyalty programs and promotions, including direct marketing rules.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Russian privacy law does not prohibit personal data transfer, including cross-border (international) data transfer. Data transfer must be formalized by a data transfer/processing agreement, demonstrating that the parties prioritize compliance with data protection laws and implement legal measures to preserve the confidentiality and security of the personal data being transferred. The agreement must contain the following elements:

(a) list of processing operations carried out by the receiving party on the personal data;

(b) security and confidentiality obligation of the receiving party;

(c) purposes of the personal data transfer; and

(d) list of security measures to be implemented by the receiving party (in accordance with Russian data protection laws).

Cross-border transfer of personal data is defined as the transfer of personal data to a foreign third party (ie, foreign individual, legal entity or state authority) abroad. Key requirements for cross-border data transfers include entering into a data processing agreement (as described above) and ensuring an appropriate legal ground to the transfer, according to the adequacy of recipient country (see below).

Legal grounds for the cross-border transfer depend on country where data is transferred. In this regard, there are jurisdictions providing adequate level of data subjects' rights protection and those which do not. "Adequate" jurisdictions are states-parties to Convention 108 (eg, EU members); and countries considered adequate by Roskomnadzor (Australia, Israel, Canada, New Zealand, Republic of Korea, Kazakhstan, Singapore, Chile, Japan etc).

Where personal data is transferred to "adequate" jurisdictions, the general approach to legal grounds applies. If a recipient jurisdiction is not considered "adequate", the scope of appropriate legal grounds is quite narrow. For example, for consent-based data transfer, the individual's written consent, subject to statutory requirements, is needed.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

In addition to the data transfer requirements set out in question 9.1, parties must take into account the data localization requirement (see question 5.1(d)), where applicable.

There are no exemptions for intra-group transfers. Subsidiaries and affiliates are considered third parties, so the general rules apply. Moreover, in practice, shared use of information systems within corporate groups constitutes data transfer, which must be compliant with the legal requirements outlined above.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Privacy-related violations may entail the following sanctions:

(a) administrative fines of up to 75,000 RUR (approx US $1,180) for personal data processing reasons, which may be imposed repeatedly if separate administrative proceedings are initiated per breach;

(b) administrative fines of up to 6 million RUR (approx US $94,100) for a first violation of the localization requirement, and of up to 18 million RUR (approx US $282,300) for a repeated offense;

(c) administrative fines of up to 500,000 RUR (approx US $7,850 USD) for advertising reasons;

(d) restriction of access (blockage) to a website or app (so that it will no longer be available to Russian citizens) in cases where personal data processing practices on such website or app are not compliant with Russian privacy laws;

(e) forced suspension of unlawful data processing activities; and

(f) criminal sanctions, such as imprisonment and fines, which may be imposed for unlawful access to computer information that results in the destruction, blockage, modification or copying of computer information, as well as for illegal disclosure of information about an individual's private life. Criminal liability may be imposed only on individuals (ie, company's officials), Russian laws do not impose criminal liability on legal entities.

10.2 Do individuals have a private right of action? What are the potential remedies?

Individuals are entitled to claim compensation for damage (including moral damages) caused by illegal processing of their personal data through the court. However, such practice is quite rare and amounts of compensation awarded to individuals are not high.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Russia which affect privacy?

Data protection rules in Russia are based on basic principles and approaches which are also relevant for the European Union (for example, purpose limitation, data minimization, etc). However, there are certain specific restrictions, which reflect policy of the state in the area of privacy and data protection.

In particular, Russian privacy regulations reflect a general localization trend. In addition to the personal data localization requirement, there are also several specific rules, eg, requiring that Russian telecom providers providing communication services under licenses, and moderators of dissemination of information on the Internet (for example, social media, messenger, etc), retain the content of users' messages and related meta-data in Russia.

The localization trend is based on certain policy considerations, such as protection of individuals' rights, effective prevention and investigation of terrorism, etc.

One more peculiarity to mention is the consent-focused approach to appropriate legal grounds. In general, Russian regulators are quite conservative in this regard and construe alternative legal grounds quite narrowly. For example, Roskomnadzor is quite skeptical about a controller's legitimate interest so, in practice, such justification applies very rarely.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Currently there are several draft laws that are widely discussed in Russia that are aimed at modernizing Russian data protection legislation in terms of consent requirements and data pseudonymization and anonymization. However, it is not yet clear when such amendments will be considered by the Russian Parliament.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Russia?

N/A.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

In the last few years, companies operating in Russia have faced new obligations related to localizing personal data in Russia. The officially articulated purpose of this initiative is improved protection of data subjects in Russia. At the same time, these measures have become a significant issue for global companies (especially data driven companies) having a presence in Russia or otherwise targeting it.

In addition, in terms of enforcement, the regulator has shifted its focus on compliance to the online environment and IT companies. This reflects a general digitalization trend, whereby an individual's daily activities have become focused on online platforms, so that communication is carried out via social media and messages, purchases are made online, etc.

12.2 What do you envision the privacy landscape will look like in 5 years?

On October 10, 2018, the Russian Federation signed a protocol modernizing Convention 108.

Russian officials have already announced elaboration of respective amendments to the Russian laws and confirmed that they will move towards harmonization with the Convention. Prospective changes may include data breach notification obligations, definitions of data processor and data recipient, new types of sensitive data, etc.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Fines for non-compliance with the localization requirement have recently come into force (see question 10.1(b). High fines of up to 18 million RUR (approx US $282,300) are expected to significantly affect the privacy landscape in Russia. If, previously, risks for companies processing the personal data of Russian citizens in cases of non-compliance with the localization requirement were rather remote (enforcement measures were limited to the blockage of the website/app), now they may become the most important issue in terms of data protection.

One more challenge faced by companies doing business in Russia relates to the rather conservative approach of Russian regulators, eg, regarding appropriate legal grounds for data processing, data pseudonymization and anonymization, etc.

Finally, data protection laws are developing worldwide. In light of this, companies and corporate groups doing business in several jurisdictions face the problem of harmonized compliance. The most noticeable issue is balancing compliance with the EU's GDPR and the Russian Personal Data Law, which is quite onerous both from legal and business perspective due to the different legal requirements and practical approaches to their implementation.

SERBIA

1 PRIVACY LAW

1.1 How is privacy regulated in Serbia?

Privacy is regulated by a number of binding laws, bylaws and other forms of regulations adopted on national level. However, by adopting a *lex generalis* last year, which is based on the EU's GDPR and Police Directive, Serbia made important steps in increasing level of data protection and reaching EU standards. It is important to emphasize that the work on privacy regulatory framework is yet to be completed. The Serbian Law on Personal Data Protection ("LPDP") states that the provisions of other laws relating to the processing of personal data are to be harmonized with the provisions of that Law by the end of 2020, and that the bylaws prescribed by the LPDP must be adopted by August 21, 2019.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The core law regulating privacy in the Republic of Serbia is the newly-adopted LPDP, based on the GDPR and Police Directive. This law regulates the right to the protection of natural persons in relation to the processing of personal data 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 others 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, such as:

(a) Information Security Law — which regulates the use of personal data in ICT systems, measures for their protection from unauthorized access, as well as the protection of the integrity, availability, authenticity and integrity of that data;

(b) Advertising Law — which regulates the necessity of obtaining a prior consent from the person whose personal good, including personal data, is contained in an advertisement. Namely, the law prescribes that in case the advertisement contains a personal good on the basis of which the identity of the person can be ascertained or recognized the advertisement message cannot be published without the prior consent of the person concerned;

(c) Law on Public Information and Media — which regulates the use of personal data in media, with special focus on the use of children's data;

(d) Criminal Code — which prescribes criminal offences related to the violation of personal data, such as breach of secrecy of letters and other means of communication, unauthorized wiretapping and recording, unauthorized photography, unauthorized publication and display of other people's files, portraits and footage, and unauthorized collection of personal information;

(e) Law on Civil Procedure and Law on Criminal Procedure — which prescribe rules related to the exclusion of the public from the judicial hearing in order to protect the interests of the minor or the privacy of parties in the proceedings; and

(f) Employment Act, Law on Records in the Field of Employment and Law on Compulsory Social Security — which regulate the collection of data of employees.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

(a) **Commissioner for Personal Data Protection**. The most important player for the privacy law enforcement is the Commissioner for Personal Data Protection ("Commissioner"), as a regulatory body. The Commissioner is a supervisory authority, which acts, in accordance with the LPDP, on the territory of the Republic of Serbia. The Commissioner supervises and enforces privacy law in accordance with its authority, promotes public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data. Additionally, the Commissioner advises the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing the data. Furthermore, the Commissioner influences the enforcement of privacy law through its authority to review and evaluate the implementation of the provisions of the law and otherwise supervise the protection of personal data by using inspection powers, as well as through its authority to impose a temporary or permanent restriction on the performance of a processing operation, including a prohibition on processing.

(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 a Commissioner concerning them, or, where the Commissioner does not render a decision within 60 days from the day of the receipt of the complaint, to initiate 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 he/she considers that the controller or processor has infringed his/her rights when processing personal data.

2 SCOPE

2.1 Which companies are subject to privacy law in Serbia?

Privacy law in Serbia applies to all companies which 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 carried out in Serbia. However, privacy law also applies to companies which 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 compensation 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Privacy law in Serbia applies to companies outside the country in the circumstances set out in question 2.1. In these cases, the company outside the country is obliged to designate, in writing, a representative in the Republic of Serbia, unless:

(a) processing is done only occasionally, it does not include to a great extent the processing of sensitive data or personal data related to convictions for criminal offenses and other offenses and is unlikely to cause risk to the rights and freedoms of individuals, taking into account the nature, circumstances, extent and purposes of processing;

(b) the controller or processor is a competent authority.

The controller or processor must authorize the representative to be a person to whom, in addition to the controller or processor, or instead of them, the data subject, the Commissioner, as the supervisory body, or a third person may address all matters relating to the processing of personal data in order to ensure compliance with the domestic law.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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. However, the processing may take place under the following conditions:

(1) If the data subject has given explicit consent to the processing of such personal data for one or more specified purposes, except where domestic law provide that the prohibition of sensitive data processing may not be lifted by the data subject;

(2) If processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by domestic law or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(3) If processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(4) If processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(5) If processing relates to personal data which is manifestly made public by the data subject;

(6) If processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

(7) If processing is necessary for reasons of substantial public interest, on the basis of domestic law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(8) If processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or the management of health or social care systems on the basis of domestic law or pursuant to the contract with a health professional, if the processing is performed by or under the supervision of a health professional or other person who has an obligation of professional secrecy prescribed by law or professional rules;

(9) If processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(10) If processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Additionally, such processing of sensitive data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, must be subject to appropriate safeguards, including organizational and technical measures, for the rights and freedoms of the data subject.

However, these obligations do not apply to processing carried out by the competent authorities for special purposes. For the sake of clarity, processing carried out by competent authorities for special purposes refers to processing done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public and national security. The processing of sensitive data

carried out by competent authorities for special purposes is only permissible if necessary, with the application of appropriate measures to protect the rights of the data subject, in one of the following cases: (a) the competent authority is authorized by law to process sensitive data; (b) the processing of sensitive data is performed in order to protect the vital interests of the data subject or other natural person; or (c) processing refers to sensitive data which data subject has clearly made available to the public.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Key privacy principles which need to be followed by companies when processing personal data are the following:

(a) **Lawfulness, fairness and transparency**, meaning that companies shall process personal data lawfully, i.e. in accordance with applicable laws, fairly and in a transparent manner in relation to the data subject;

(b) **Purpose limitation**, meaning that companies shall collect personal data for specified, explicit and legitimate purposes and not further process them in a manner that is incompatible with those purposes;

(c) **Data minimization**, meaning that personal data processed by companies shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) **Accuracy**, meaning that personal data processed by companies shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) **Storage limitation**, meaning that personal data processed by companies shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(f) **Integrity and confidentiality**, meaning that companies shall process personal data 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.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

In general, there is a difference between companies which act as controllers and the ones that act as processors:

Companies acting as controllers. These companies determine the purpose, and the method of the data processing and shall be responsible for and be 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.

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. More precisely, the contract or other legal act must stipulate that the company acting as processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by law; in such a case, the processor must inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all appropriate technical and organizational measures to ensure a level of security for the rights and freedoms of natural persons;

(d) respects the conditions for engaging another processor, meaning that processor cannot engage another processor without the prior specific or general written authorization of the controller. In the case of general written authorization, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes;

(e) assists the controller by appropriate technical and organizational measures, insofar as this is possible, taking into account the nature of the processing, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;

(f) assists the controller in ensuring compliance with the obligations related to the security of processing, notification of a personal data breach to the supervisory authority and data subject, data protection impact assessment and prior consultation, taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless law requires storage of the personal data; and

(h) makes available to the controller all information necessary to demonstrate compliance with its obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by 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 when data breach takes place without undue delay.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Key obligations required by privacy law include the following:

(a) **Posting a privacy policy.** There is no specific obligation required by national law to post a privacy policy as such. However, there is an obligation of the controller to provide the data subject, at the time when personal data are obtained, with all of the necessary information related to processing, such as the identity and the contact details of the controller, the purposes of the processing, the contact details of the data protection officer, where applicable, etc. The information must be provided without undue delay in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

(b) **Keeping records of processing operations.** Both 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, which must contain all of the following information:

(i) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(ii) the purposes of the processing;

(iii) a description of the categories of data subjects and of the categories of personal data;

(iv) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;

(v) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, the documentation of suitable safeguards where needed;

(vi) where possible, the envisaged time limits for erasure of the different categories of data; and

(vii) where possible, a general description of the technical and organizational security measures adopted for securing rights and freedoms of natural persons.

Similar records must be kept by each processor/processor's representative with regard to all categories of processing activities carried out on behalf of a controller.

These records must be in writing, including in electronic form. However, there is an exception to the obligation of keeping records of processing operations in cases where: (1) controller and processor are companies or organizations with less than 250 employees, unless the processing carried out by them may cause a high risk to the rights and freedoms of the data subject, (2) processing is not occasional or (3) processing includes special categories of personal data, including that related to criminal convictions, criminal offenses and security measures.

(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. A data protection risk impact assessment is especially required in the case of:

(i) 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;

(ii) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or

(iii) a systematic monitoring of a publicly accessible area on a large scale.

If the risk impact assessment indicates that the processing would result in a high risk, in the absence of measures taken by the controller to mitigate the risk, the controller is obliged 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:

(i) for courts acting in their judicial capacity;

(ii) where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(iii) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

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 the data breach.** The controller is obliged to notify a personal data breach to the Commissioner as the 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Serbia? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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.

Also, the data protection officer can play an important role, since he/she informs and gives an opinion to the operator or processor, as well as employees who perform processing operations, on their legal obligations regarding the protection of personal data.

In the end, there is also an obligation of the company acting as controller to seek prior consultation with Commissioner as supervisory authority in cases where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. The Commissioner will be obliged to issue an opinion related to this question.

There are no specific resources allocated by the state, for the purpose of helping companies address these obligations.

6.2 How are data breaches regulated in Serbia? What are the requirements for responding to data breaches?

If a data breach occurs, the law prescribes obligations for both controller and processor. 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.

The processor is obliged to inform the controller without undue delay after becoming aware of such breach.

In cases where a data breach has taken place, the law provides various legal remedies aimed at addressing such breaches:

(a) **Right to lodge a complaint with the Commissioner.** A data subject has a right to lodge a complaint with the Commissioner, if he/she considers that the processing of personal data relating to him/her infringes the national law regulating privacy. 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 he/she considers that the controller or processor has infringed his/her rights when processing the data subject's 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 him/her 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.

In addition to legal remedies, 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals have the following rights with respect to their personal data:

(a) **Right to be informed.** This right correlates to the controller's obligation to provide, at the time when personal data is obtained, the data subject with all necessary information. The information must be provided without undue delay in a concise, transparent, intelligible and easily accessible form, using clear and plain language. However, in cases where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either charge a reasonable fee taking into account the administrative costs of providing the information or refuse to act on the request. Depending whether processing is carried out by competent authorities for special purposes or not, the list of information which needs to be provided to the data subject will differ. When processing is not carried out for special purposes, the information which needs to be provided includes, inter alia, the following:

(i) the identity and the contact details of the controller and, where applicable, of the controller's representative,

(ii) the contact details of the data protection officer, if such person has been appointed,

(iii) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,

(iv) the recipients of the personal data, if any,

(v) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,

(vi) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, etc.

All this information, with small exceptions, must also be provided where personal data has not been obtained from the data subject directly.

Where processing is carried out by competent authority for special purposes (see question 3.2), the information set out in (iii), (iv) and (v) may be limited, or not provided at all, though only to the extent and for the duration necessary and proportionate.

(b) **Right of access.** Data subjects have right to obtain confirmation from the controller as to whether or not personal data concerning them is being processed, and to have access to the personal data and relevant information related to the processing. Depending whether processing is carried out by competent authorities for special purposes or not, the right to access to certain information related to processing will differ.

(c) **Right to rectification.** This is the right of the data subject to obtain, from the controller without undue delay, the rectification of inaccurate personal data concerning him/her. Taking into account the purposes of the processing, this right also includes the right of the data subject to have incomplete personal data completed, which could include the provision of a supplementary statement.

(d) **Right to erasure.** This is the right of the data subject to obtain from the controller the erasure of personal data concerning him/her without undue delay. Depending whether processing is carried out by competent authorities for special purposes or not, the right to access to certain information related to processing will differ.

(e) **Right to restriction of processing.** The data subjects have the right to obtain from the controller restriction of processing. Depending whether processing is carried out by competent authorities for special purposes or not, the right to access to certain information related to processing will differ.

(f) **Right to data portability.** This right comprises of the right of the data subject to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit such data to another controller without hindrance from the controller to which the personal data had been provided, where the processing is based on consent and is carried out by automated means. In addition, this right includes the right of the data subject to have the personal data directly transmitted from one controller to another, where this possibility is technically feasible. However, the right to data portability cannot be enforced when 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. In addition, it shall be noted that the enjoyment of this right must not adversely affect the rights and freedoms of others. This right to data portability does not apply to the processing carried out by competent authority for special purpose.

(g) **Right to object.** As regards the right to object, the data subject has the right to object, on grounds relating to his/her particular situation, at any time to processing of personal data concerning him/her in cases when processing is carried out for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or when processing is carried out for the purposes of legitimate interests pursued by the controller or by a third party, including profiling based on these grounds. In addition, data subjects have right to object, on grounds relating to their particular situation, when their personal data is processed for scientific or historical research purposes or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest. Right to object may be exercised by automated means using technical specifications in cases when there is a use of information society services included. Once the data subject objects, the controller may no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

When it comes to processing done for direct marketing purposes, data subjects have the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. The right to object must be explicitly brought to the attention of data subject at the time of the first communication with the data subject at the latest, and must be presented clearly and separately from any other information.

(h) **Right not to be subject to a decision based solely on automated processing, including profiling.** Data subjects have this right where the decision produces legal effects concerning them or similarly significantly affects them. Depending on whether processing is carried out by competent authorities for special purposes or not, the enjoyment of this right by a data subject will vary.

Data controllers must facilitate the exercise of data subject rights and provide information on action taken regarding a request to the data subject 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The main requirement for processing of personal data for the purpose of sending direct marketing communications such as push notifications, emails or mobile text messages is informed consent of the data subject. The data subject must be informed on:

(a) all aspects of marketing communications which involve processing of his/her personal data (eg, e-mail address, telephone number etc.),

(b) the scope of the marketing communication, and

(c) his/her 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 not, in any way, impacting processing done before the moment of revocation of consent.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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).

Furthermore, visitors must also be given an opportunity to inform themselves on all aspects of usage and activation/deactivation of cookies on the website, such as:

(a) what are cookies?

(b) which types of cookies exist, and which cookies are active on the site?

(c) what types of data do they gather exactly, and what is their purpose?

(d) how is personal data of visitors used etc?

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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

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.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

In order to share data with any third parties for the purpose of customer matching and audience building, advertisers must comply with the general rules of the LPDP.

First and foremost, advertisers must have, as a legal basis for every processing activity involved in customer matching, including data sharing for the purpose of customer matching and audience building, clear and informed consent obtained directly from the data subjects. The notice in this case must, as any other standard privacy notice, present all relevant information regarding the processing/sharing of personal data of data subjects in a clear and transparent manner.

Data subjects must also be made aware of the fact that they can revoke their consent freely, at any time, and without meeting any special requirements, and of the means of revocation.

8.5 Are there specific privacy rules governing data brokers?

There are no particular rules that govern data brokers; therefore, the general rules on personal data protection apply.

8.6 How is social media regulated from a privacy perspective?

Social media is not explicitly regulated by the Serbian legal system, therefore the general rules on personal data protection apply.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

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, such as:

(a) basic information about the controller;

(b) which personal data is being collected;

(c) the existence of the controller's legitimate interest for processing (if it exists);

(d) how is the personal data collected;

(e) what is the legal basis for processing;

(f) what is the purpose of personal data processing;

(g) how is the personal data stored and what data security measures are implemented;

(h) what are the rights of data subjects with regards to processing of their personal data by the controller, with special attention to their right of revocation of consent for personal data processing;

(i) who else besides the controller has access to their personal data;

(j) is the personal data transferred outside the country;

(k) for how long their personal data is stored by the controller;

(l) what data security measure have been implemented;

(m) contact information of the controller's data protection officer ("DPO"); and

(n) any other relevant information.

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.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Data transfer under the LPDP is governed by a slightly different set of rules then those contained in the GDPR. Although most essential parts remain the same, there are some specific differences than need to be pointed out.

The transfer can be done in the following cases:

(a) Transfer based upon the adequate level of protection: Ie, 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 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, have prescribed either the 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), it is not precisely prescribed which are the competent authorities that are authorized to perform that kind of processing, and therefore the transfer. For that reason, its 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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Article 67 of the LPDP allows companies to pass so-called "binding corporate rules" 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 binding corporate rules 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 the all these conditions are fulfilled, the Commissioner will approve binding corporate rules 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.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Under the LPDP, controllers and processors can be fined between 5,000–2,000,000 RSD (approx 40–16,900 EUR) 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.

The Law on Information Security also prescribes that a fine of RSD 50,000.00–2,000,000.00 may be imposed on the 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.

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 individuals have a private right of action? What are the potential remedies?

A data subject has the right to file a complaint with the Commissioner if he/she considers that the processing of his/her personal data has been carried out contrary to the provisions of the LPDP. Filing a complaint with the Commissioner does not affect this person's right to initiate other administrative

or judicial protection proceedings, eg, filing lawsuits before the national civil courts and filing lawsuits to administrative courts against the Commissioner's decision. The same rule applies to all other cases of seeking administrative or judicial protection.

Furthermore, the data subject, the controller, the processor, or other natural or legal person to whom the Commissioner's decision applies, may initiate an administrative dispute against that decision within 30 days from the day of receiving the decision. If the Commissioner does not act on the complaint or fails to act within 60 days from the day of filing the complaint, the data subject has the right to initiate an administrative dispute.

The data subject is also entitled to judicial protection if he/she believes that the LPDP has been violated by the controller or processor by the processing of his/her personal data.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Serbia which affect privacy?

There are no rules that are particular to the culture of Serbia which affect privacy.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

As the new LPDP has only recently been adopted and began to apply as from August 21, 2019, numerous theoretical, practical and legal clarifications should be expected in the coming period.

All bylaws envisaged by the LPDP are to be adopted by May 21, 2020, and the provisions of other laws relating to the processing of personal data are to be harmonized with the provisions of the LPDP by the end of 2020.

In which direction these clarifications and harmonization will go, and where will it start, remains to be seen.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Serbia?

The new 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.

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.

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 you observed over the past few years? In your opinion, what propelled/triggered these changes?

In the area of personal data protection, the only major recent development has been the adoption of the new LPDP in 2018. The new LPDP offers fresh updates and solutions to existing problems not covered by the previous Law and brings the Serbian legal system one step closer to harmonization with the legal system of the European Union.

Also worthy of note, many other laws adopted in the past few years have paid much closer attention to personal data protection in their respective areas, going so far as to prescribe special rules to strengthen and specify existing personal data protection procedures.

The main reason for these changes is Serbia's aspiration to become a full-fledged member of the European Union, as well as to create a safer, more regulated and stable environment for the flow and processing of personal information of its citizens.

12.2 What do you envision the privacy landscape will look like in 5 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.

12.3 What are some of the 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 new LPDP in Serbia is the harmonization of the companies' internal documentation, acts and procedures.

Given the fact that the new 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 new LPDP has only recently been adopted, 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 new LPDP will companies be able to conduct their business in line with data protection rules and procedures with greater certainty.

SINGAPORE

1 PRIVACY LAW

1.1 How is privacy regulated in Singapore?

There is no overarching legislation in Singapore which governs the regulation of privacy. Be that as it may, there are laws which regulate, inter alia, the access to and the processing of personal data, in addition to sector-specific legislation, including, but not limited to, the following:

(a) Personal Data Protection Act 2012 (No 26 of 2012) ("PDPA");

(b) Banking Act (Cap. 19);

(c) Central Provident Fund Act (Cap. 36);

(d) Computer Misuse Act (Cap. 50A);

(e) Cybersecurity Act 2018 (No 9 of 2018);

(f) Electronic Transactions Act (Cap. 88);

(g) Official Secrets Act (Cap. 213);

(h) Spam Control Act (Cap. 311A) ("SCA");

(i) Statistics Act (Cap. 317);

(j) Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319); and

(k) Telecommunications Act (Cap. 323).

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

See question 1.1. In addition, the main obligations that parties (including, but not limited to, advertisers) will need to comply with under the PDPA are set out below:

(a) **Consent**: Parties may collect, use or disclose personal data for purposes for which an individual has given his/her consent, 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 for any purpose, parties must cease such collection, use or disclosure of the personal data for such purpose.

(b) **Notification**: 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) **Purpose**: 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 the individual to consent to the collection, use or disclosure of his/her personal data beyond what is reasonable to provide that product or service.

(d) **Withdrawal of consent**: While not specifically required under the PDPA, it is considered prudent practice to expressly inform the individual that he/she may withdraw consent to the use of his/her personal data (not limited to the receiving of promotional/advertising materials from the parties) and the manner in which such withdrawal should be

communicated to the parties. Parties are required by law to cease any collection, use or disclosure of the personal data for any purpose for which consent has been withdrawn.

(e) **Sharing of personal data**: Parties need to comply with the PDPA regardless of where the personal data is transferred. This also applies to parties transferring data outside Singapore to related entities within a group. As such, parties should engage the parties to which they transfer data in order to provide for the protection of personal data outside Singapore, so that the standard of protection of personal data so transferred is comparable to the protection under the PDPA.

(f) **Disclosure of personal data to third parties**: An organization is considered a data intermediary if it processes data on behalf of another organization. Where an individual discloses information to third parties by/through a website, if any of the parties' related entities or third parties process such personal data as a data intermediary pursuant to a contract with the third parties evidenced or made in writing, the parties will remain liable for the protection and retention of personal data so disclosed.

(g) **Disclaimer of liability for unauthorized access**: Under the PDPA, parties are statutorily required to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. Such liability cannot be wholly disclaimed if reasonable measures for protection of personal data have not been taken. Under the PDPA, both parties and their officers can be held liable for any breach of the provisions of the PDPA.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The PDPA confers various powers on the Personal Data Protection Commission ("PDPC") to enforce provisions of the PDPA. These powers may generally be categorized as follows:

(a) **Powers relating to 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 action to ensure its compliance.

(b) **Powers relating to review**: The PDPC is empowered to review an organization's reply to a request made by an individual authorized under the PDPA and to confirm the organization's reply or direct the organization to take certain action in relation to the individual's request.

(c) **Powers relating to alternative dispute resolution**: These powers generally relate to the manner in which a complainant and an organization may resolve the complaint, eg, through mediation or other modes of dispute settlement.

2 SCOPE

2.1 Which companies are subject to privacy law in Singapore?

The provisions of the PDPA apply to all persons and entities, however, they do not impose any obligations on:

(a) any individual acting in a personal or domestic capacity;

(b) any employee acting in the course of his 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.

Further, business contact information is not covered under the provisions of the PDPA.

2.2 Does privacy law in Singapore apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Singapore?

Section 2 of 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.'

Indeed, 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The PDPA does not expressly draw a distinction between different types of personal data. Further, the PDPA does not define "sensitive personal data". Be that as it may, the Advisory Guidelines on Key Concepts in the Personal Data Protection Act published by the PDPC, recognizes that more stringent measures may be required for organizations to meet their obligations in respect of sensitive personal data. The Guidelines also specify that it would be an aggravating factor for organizations handling sensitive personal data not to have adequate safeguards to protect such data from the harm that may result from its disclosure.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Please refer to the preceding paragraphs.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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 the data protection provisions of the PDPA which relate to the protection and retention of personal data, and not to any of the other data protection provisions.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Organizations are required to comply with the following obligations, inter alia:

(a) consent;

(b) purpose limitation;

(c) notification;

(d) access and correction;

(e) accuracy;

(f) protection;

(g) retention limitation;

(h) transfer limitation; and

(i) accountability (including the appointment of a data protection officer, and the development and implementation of data protection policies and practices).

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Singapore? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Section 24 of 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 and/or similar risks. 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, eg, 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.

Further guidance can be obtained from the Advisory Guidelines on Key Concepts in the Personal Data Protection Act published by the PDPC; it might 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 may be considered:

- the size of the organization and the amount and type of personal data they hold;
- who within the organization has access to the personal data; and
- whether the personal data is/will be held or used by a third party on behalf of the organization.

6.2 How are data breaches regulated in Singapore? What are the requirements for responding to data breaches?

Currently, there are no mandatory data breach notification requirements under the PDPA. Be that as it may, the PDPC recently published a revised Guide to Managing Data Breaches 2.0, which indicates that the PDPC intends to introduce a mandatory data breach notification requirement under the PDPA in the near future.

Under the revised Guide, 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 is of 'significant scale'. Further, organizations are advised to assess whether a potential breach meets this reporting threshold expeditiously, albeit within 30 days from learning of a potential data breach.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The PDPA recognizes the rights of individuals to protection their personal data, including, but not limited to, the right of access and correction of the data.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The PDPC maintains a Do Not Call Register. Generally, prior to sending a marketing SMS to a Singapore telephone number (where the subscriber is an individual), an entity must apply to the Do Not Call Registry ("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/MMSs and fax messages do not fall within the ambit of the Registry. Hence, it is permissible for parties to send B2B SMSs without fulfilling these requirements, where the subscriber of the number is a corporate entity and not an individual. However, often the subscribers enlisted with the telcos are individuals and not the corporate entities which employ the subscribers. Ascertaining whether each of the numbers to which the SMS will be sent are registered in the name of an individual or a corporate entity is likely to be cumbersome. Hence, the safe and easier alternative will be to carry out the check on the Register and/or obtain unambiguous consent from the individual, prior to sending a marketing SMS.

The Registry allows subscribers of Singapore telephone numbers to opt out of marketing calls, SMSs and faxes to their numbers by registering in any or all three Do Not Call Registers (ie, the No Voice Call Register, the No Text Message Register and the No Fax Message Register). As mentioned above, parties should apply to the Registry to confirm whether the number is listed in the respective Register. If parties have an on-going relationship with a subscriber of a Singapore telephone number (and have obtained clear and unambiguous consent), they may send marketing SMSs to the number without checking with the Registry. Each exempt SMS must contain an opt-out facility that the subscriber can use to opt out from receiving such an SMS. If a subscriber opts out, the parties can no longer rely on the exemption and must stop sending further marketing SMSs to the number, within 30 days.

The Do-Not-Call framework set out in the PDPA covers only telephone calls, SMSs, and faxes. It does not include emails and mail delivered by post. Hence, in order to circumvent the onerous requirements of the PDPA, organizations can consider sending emails instead of SMSs (although this may be slightly less effective from the marketing perspective). However, prior to sending marketing emails, parties need to ensure that they comply with the requirements set out in the SCA, which sets out requirements in relation to the sending of unsolicited commercial electronic messages in bulk. The requirements of the SCA can be considered to be less onerous when compared to the PDPA.

The SCA stipulates that the following must be complied with:

(a) the title in the subject field should not be false or misleading as to the content of the message;

(b) the letters "<ADV>" with a space before the title in the subject field (or if there is no subject field, in the words first appearing in the message) should be set out to clearly to identify that the message is an advertisement;

(c) the header information should not be false or misleading; and

(d) an accurate and functional email address or telephone number by which the sender can be readily contacted should be set out.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The PDPA also applies to the collection, use, or disclosure of personal data using cookies and other tracking technologies. The Advisory Guidelines on the Personal Data Protection Act for Selected Topics published by the PDPC provide as follows:

(a) The obligation to obtain the individual's consent for the collection of his personal data rests with the organization that is collecting such personal data, whether by itself or through its data intermediaries.

(b) Where an organization operates a website which a third party uses to collect personal data, and the website operator itself is not collecting such personal data, the obligation is on the third-party organization to obtain the consent required to collect such personal data.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The PDPA also applies to targeted advertising and behavioral advertising. Where targeted advertising and behavioral advertising involve the collection and use of personal data, the individual's consent must be obtained.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Under the PDPA, organizations must notify an individual of the purposes of the collection, use and disclosure of personal data, before collecting the same, and have obtained consent. If organizations intend to share personal data for a different purpose from the original purpose for which consent has been obtained, they must inform the individuals of the new purpose and obtain fresh consent.

8.5 Are there specific privacy rules governing data brokers?

The general principles enunciated in the PDPA apply with equal effect to data brokers.

8.6 How is social media regulated from a privacy perspective?

The Advisory Guidelines on the Personal Data Protection Act for Selected Topics published by the PDPC provides 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 are newspapers, telephone directories and websites containing content which is generally available to the public. Where social networking sources are publicly available, the PDPA does not prohibit organizations from collecting personal data about an individual without his/her consent. Please refer to the section on "The Consent Obligation" in the Key Concepts Guidelines for more explanation of the 'publicly available data' exception.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

The general principles enunciated in the PDPA apply with equal effect to loyalty programs and promotions.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Section 26 of the PDPA limits the ability of an organization to transfer personal data outside Singapore. Specifically, Section 26(1) of the PDPA provides that an organization must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organizations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

An organization may transfer personal data overseas if it has taken appropriate steps to ensure that it will comply with the data protection provisions in respect of the transferred personal data while such personal data remains in its possession or under its control; and if the personal data is transferred to a recipient in a country or territory outside Singapore, that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Please see question 9.1.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 to direct an organization to pay a financial penalty, the PDPC will take into account the seriousness of the incident 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;

(ii) whether the organization had acted deliberately or willfully;

(iii) whether the organization had known or ought to have known the risk of a serious contravention and failed to take reasonable steps to prevent it;

(iv) extent of non-compliance in terms of the PDPA obligations that the organization had failed to discharge;

(v) number of individuals whose personal data had been subjected to harm and risks as a result of the breach;

(vi) whether the organization had appointed a 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 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, and that the individuals had accepted the remedy; and
- whether the organization admitted to liability for the data breach.

10.2 Do individuals have a private right of action? What are the potential remedies?

The PDPA provides individuals with the right to commence a private action against an organization where such an individual has suffered loss or damage as a direct result of non-compliance by the organization of the data protection provisions under the PDPA, subject, of course, to certain limitations. Be that as it may, where the PDPC has issued a decision under the PDPA in respect of such a contravention, the right to commence a private action is only exercisable after the decision issued by the PDPC becomes final and 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Singapore which affect privacy?

No

11.2 Are there any hot topics or laws on the horizon that companies need to know?

As mentioned in question 6.2, changes are anticipated in the near future in relation to the data breach notification requirements and obligations.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Singapore?

- It is imperative to have a comprehensive data protection policy in place.
- Appoint a data protection officer.
- Carry out periodic audits.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The enactment of the PDPA in 2012 has ushered in much-needed changes to the privacy landscape in Singapore. The need to create a balance between the need to protect individuals' personal data against organizations' need to obtain and process such data for legitimate purposes, propelled the above.

12.2 What do you envision the privacy landscape will look like in 5 years?

The Singapore regime is likely to move towards a GDPR-like regulatory regime over the next few years.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The law struggles to keep pace with the advancement of technology. Similarly, companies constantly struggle to keep pace with technological advancements whilst balancing the obligations set out in existing legislation. Be that as it may, the PDPC has done a commendable job in educating all stakeholders, and constantly attempting to disseminate guidance and information pertaining to the PDPA and the regulatory regime.

SOUTH AFRICA

1 PRIVACY LAW

1.1 How is privacy regulated in South Africa?

Dedicated data protection legislation is not yet in force in South Africa and thus privacy law is dealt with on a piecemeal basis by various pieces of legislation.

A dedicated data protection law in the form of the Protection of Personal Information Act 2013 ("POPI") has been promulgated but is not yet in force. The answers to the questions which follow will be with reference to the data protection system that will be put in place by POPI, as well as to current legislation that covers the same to a limited extent.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

(a) The Consumer Protection Act 2008 ("CPA") contains some specific provisions relating to direct marketing and consumer privacy.

(b) The National Credit Act 2005 ("NCA") regulates the privacy of credit information.

(c) The Electronic Communications and Transactions Act 2002 ("ECTA") contains certain voluntary data protection provisions in the context of electronic communication.

(d) The Promotion of Access to Information Act 2000 ("PAIA") regulates access to information held by public and private bodies.

(e) The right to privacy is also enshrined in section 14 of the Constitution of the Republic of South Africa, 1996 (the "Constitution").

(f) Once POPI is in enforce it will be the key legislation regulating privacy to the extent that there is no other legislation already existing which provides a greater protection to privacy than POPI.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

POPI establishes the office of the Information Regulator, which will be responsible for overseeing the protection of personal personally identifiable information.

2 SCOPE

2.1 Which companies are subject to privacy law in South Africa?

POPI applies to the processing of information by or for a responsible party (including a company) domiciled or established in South Africa.

2.2 Does privacy law in South Africa apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

POPI applies to a responsible party domiciled outside the country only if the processing uses automated or non-automated means situated in South Africa, unless those means 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 POPI to apply.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in South Africa?

"Personal Information" is defined in POPI 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

POPI provides for a category of "special personal information" that is afforded a higher degree of protection by prohibiting the processing of this information unless the specific circumstances listed in POPI are present. Special personal information is information relating to the religious or philosophical beliefs, race or ethnic origin or trade union membership, political persuasion, health or sex life or biometric information of a data subject, or criminal behavior of a data subject 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.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

POPI provides for eight key information processing principles, which form the core of the legislation:

(a) Accountability — an obligation is placed on the responsible party to ensure that the principles for key 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 POPI.

(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 POPI.

(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 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 the name and address of the responsible party, the information being collected and whether the supply of the information by the responsible party is voluntary or

mandatory. In addition, this principle sets out that personal information may only be processed by a responsible party that has notified the Information Regulator.

(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 access information held by a responsible party or which has been made available to a third party, to request a responsible party to delete inaccurate, irrelevant and unlawfully obtained information, and to request that a responsible party delete information which the responsible party is no longer authorized to retain.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

POPI 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

When POPI comes into force, a responsible party will need to provide data subjects with a notice relating to its processing of personal information. Generally, this will be in the form of a privacy policy that will be displayed on the responsible party's website.

POPI will require a responsible party to appoint an information officer, who will need to be registered with the Information Regulator.

Under POPI, a responsible party will not need to register with the Information Regulator in order to process personal information. However, it will need prior authorization from the Information Regulator in certain instances, for example when it intends to transfer special personal information or children's personal information to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in South Africa? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

POPI requires a responsible party to secure the integrity of personal information in its possession by taking appropriate, reasonable technical and organization measures to prevent any loss or unauthorized destruction, unlawful access 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.

6.2 How are data breaches regulated in South Africa? What are the requirements for responding to data breaches?

A security compromise occurs when personal information has been accessed or acquired by any unauthorized person. POPI 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 is 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 the 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

POPI affords the data subject 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 data subject no longer has the authority to be in possession or control of the personal information.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The CPA and the ECTA regulate direct marketing in South Africa on an opt-out basis. The CPA provides consumers with the right to restrict unwanted direct marketing by requiring any person who approaches the consumer for purposes of direct marketing, within a reasonable time, to desist from initiating any further communication. The ECTA provides that the sender of unsolicited communications must provide the recipient with the option to stop such communications. At the recipient's request, the sender must also provide the recipient with identifying particulars of the source from whom the sender obtained the recipient's personal information.

When POPI comes into force, direct marketing will be regulated on an opt-in basis. Processing of personal information for the purpose of direct marketing will be prohibited unless the data subject consents to such processing or the data subject is a customer of the responsible party. Even if the data subject is a customer of a responsible party, the information may still only be processed in specific circumstances such as where the purpose of the direct marketing is the marketing of the responsible party's own similar products or services. In addition, any communication initiated for the purpose of direct marketing must contain details of the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send a request that such communication must cease.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Tracking technologies such as cookies are not specifically regulated in South Africa; however, the principles of POPI will apply once it is in force, even though this aspect is not directly addressed by POPI.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

This is not specifically regulated in South Africa; however, the principles of POPI will apply once it is in force, even though this aspect is not directly addressed by POPI.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

This is not specifically addressed in POPI. However, the responsible party must ensure that the sharing of data must be in accordance with the obligations imposed by POPI once it is in force.

8.5 Are there specific privacy rules governing data brokers?

POPI does not contain provisions relating directly to data brokers.

8.6 How is social media regulated from a privacy perspective?

In the same fashion as other customer information, any and all information collected via social media will be governed by POPI.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs process a lot of information and thus will also be governed by all the principles of POPI 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 client that their information will be used for this purpose.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

POPI 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 POPI;

(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.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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 POPI provides for specific circumstances in which data may be transferred to a third party based in a foreign country, a subsidiary in South Africa may 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.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

A person convicted of an offence in terms of POPI can be sanctioned with a fine and/or imprisonment. In a case where the offender has hindered, obstructed or unlawfully influenced the Information Regulator, the term of imprisonment may not exceed 10 years. In any case, the imprisonment period

may not exceed 12 months. POPI also provides for the imposition of an administrative fine, which may not exceed ZAR10 million.

10.2 Do individuals have a private right of action? What are the potential remedies?

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 costs of lawsuit.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of South Africa which affect privacy?

There are currently no rules particular to the culture of South Africa which affect privacy.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Currently, POPI is the main focus on the privacy scene in South Africa.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in South Africa?

In most jurisdictions, "personal information" is limited to the personal information of natural persons (humans). However, POPI's definition extends to the personal information of juristic persons (including companies). This means that responsible parties will need to comply with POPI's requirements when they process personal information of both natural persons and juristic persons.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The publishing of POPI in 2013 marked a significant change in the privacy landscape. Prior to this, South Africa had no dedicated data protection legislation. Although the majority of POPI's provisions are not yet in force, companies are focusing on their data protection compliance in order to ensure that they are ready when POPI becomes law.

12.2 What do you envision the privacy landscape will look like in 5 years?

It is likely that POPI will be in force in 5 years' time. Organizations will be more focused on privacy compliance, in order to adhere to POPI'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.

12.3 What are some of the 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 to human resources and service providers. This may be particularly burdensome for small businesses, especially since organization will need to monitor, upgrade and invest in their technology on a constant basis in order to ensure that they remain complaint.

SWITZERLAND

1 PRIVACY LAW

1.1 How is privacy regulated in Switzerland?

Switzerland's federal structure characterizes the organization of the Swiss legal and court systems. The Swiss Federal Constitution ("SFC") attributes the power to legislate in civil law (including civil procedure law) and criminal law (including criminal procedure law) matters to the Federation. Hence, the core legal rules relating to privacy law are codified in Federal statutes.

The SFC provides a constitutional right to privacy. Article 13 SFC protects the right to privacy in personal or family life and in a person's home. Article 28 of the Civil Code ("CC") and the Swiss Federal Data Protection Act ("FDPA") 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 FDPA.

The FDPA is currently under revision. The aim of the revision is, primarily, to align the FDPA's standard of protection with the standard of protection offered by the European Union's General Data Protection Regulation ("GDPR"). Where appropriate, the answers below are based on the near-final text of the revised FDPA ("rev-FDPA").

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. The Cantons, too, are revising (or have already revised) their respective data protection acts.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The FDPA is the key law regulating privacy. 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.

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, eg, patient personal data, bank customer data or smart meter (personal) data. Sector-specific rules typically supersede the provisions of the FDPA. The Ordinance on the FDPA ("FDPO") is a governmental (Federal Council) ordinance that regulates more specifically certain aspects of the FDPA, eg, specifics of notification requirements or the right of access.

Swiss data protection law is rooted in the civil law protection of personality rights provided by Article 28 of the CC. In essence, the data processing principles set out in the FDPA (including purpose limitation, data minimization, storage limitation, transparent and fair processing, data accuracy, and data security) provide for protection against infringements of personality rights (data privacy) through excessive use of personal data (ie, information that identifies an individual directly or

indirectly). Article 28 of the CC remains relevant, from a privacy law perspective, where libel, slander or defamation is the concern. Furthermore, it is relevant for the protection of personality rights of legal entities. The current FDPA also governs the processing of personal data about legal entities, but the rev-FDPA will do away with this particularity of Swiss data protection law. It will cover only the processing of data that identifies individuals or renders individuals identifiable.

In addition to criminal liability governed by the FDPA, a number of provisions of the Swiss Criminal Code ("CrC") are relevant in a privacy context. These include criminal law protection of a person's reputation against defamation (including libel and slander) and criminal law provisions prohibiting unauthorized recording of private conversations or wiretapping.

Lastly, the Swiss Federal Act on Unfair Competition ("UCA"), which provides a right of action against the disparagement of competitors and their products or services, may be relevant in a privacy context.

The general framework provided by the FDPA, FDPO, CC, CrC and UCA also applies in an advertising context. In addition, the Principles issued and supervised by the Swiss Commission for Fairness in Commercial Communication, a self-regulatory body promoting fair trade practices in advertising and commercial communication, contain data 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 FDPA and the FDPO provide to that end.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The Swiss Federal Data Protection and Information Commissioner ("FDPIC") enforces the substantive provisions of the FDPA and the FDPO against businesses and organizations, as well as against Federal public authorities. Under the current FDPA, the FDPIC may only issue non-binding recommendations. However, where the business, organization or Federal authority concerned does not agree to implement the recommendation, the FDPIC may file a complaint with the Federal Administrative Court and request that the court order the defendant to implement the recommendation.

Under the current FDPA, the FDPIC may only open investigations if the privacy of a large number of persons has been or may be infringed. The rev-FDPA strengthens the FDPIC's competences. Once the rev-FDPA comes into force and applicable (this is unlikely to be before the end of 2020), the FDPIC will be able to open an investigation ex officio or upon receipt of a complaint if there are indications of an infringement of data protection obligations under the rev-FDPA.

Under the rev-FDPA, the FDPIC will have the power to issue binding decisions: The FDPIC may require the respective business or organization to correct, suspend or cease certain processing of personal 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 ("DPIA"). In contrast to supervisory authorities in most jurisdictions where the GDPR is enforced, the FDPIC will not, however, have the power to impose administrative fines on businesses or organizations. Nor will the FDPIC have the power to issue fines against individuals.

State prosecutors of the Cantons enforce criminal law provisions under the FDPA against liable natural persons (and businesses under certain circumstances). They will continue to do so under the rev-FDPA (see question 10.1). State prosecutors also enforce the privacy law-related offences under the CrC and the criminal law provisions of the UCA (see question 1.2).

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.

Furthermore, private enforcement plays a role in the enforcement of the FDPA, in particular in connection with access rights and other individual rights of data subjects. See further question 10.2.

2 SCOPE

2.1 Which companies are subject to privacy law in Switzerland?

The FDPA 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 uses.

2.2 Does privacy law in Switzerland apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The principle of effects determines the FDPA's territorial scope; in other words, the FDPA applies to the processing of personal data that has actual or potential effects in Switzerland. This includes processing activities that are conducted or initiated outside of Switzerland but actually or potentially adversely affect the privacy rights of individuals in Switzerland.

According to established case law, this territorial scope already applies to investigation proceedings of the FDPIC under the current FDPA, and may apply, in accordance with the principle of effects under private international law, in private enforcement actions. The rev-FDPA will codify the principle of effects directly in the rev-FDPA.

Under the rev-FDPA, controllers established outside of Switzerland will have to appoint a representative in Switzerland under certain conditions. In accordance with the current draft of the rev-FDPA, controllers will be required 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.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Switzerland?

The FDPA applies to the processing of personal data. It 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 identification indirectly by reference to additional information (eg, email address, telephone number, social security number or customer number).

The current FDPA governs the processing of personal data of both natural persons and legal entities. The rev-FDPA will do away with this Swiss particularity. It defines personal data as any information relating to an identified or identifiable natural person.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The FDPA considers the following categories of personal data "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; and

(d) personal data concerning administrative or criminal proceedings and sanctions.

These categories of personal data will continue to be considered sensitive under the rev-FDPA. The rev-FDPA will add two new categories:

(e) genetic data that uniquely identifies an individual; and

(f) biometric data that uniquely identifies an individual.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The following are key privacy principles that companies 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).

These principles are set out in FDPA (Articles 4–7). They will remain the key privacy principles under the rev-FDPA. A summary of these key privacy principles is set out in question 5.1.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The rev-FDPA will distinguish controllers and processors. Similarly, the current FDPA distinguishes owners of data filing systems and third parties processing on behalf of the owner.

The term "controller" (under the rev-FDPA) refers to the business, organization, natural person or Federal authority that determines (alone or jointly with others) the purpose and means of the processing of personal data.

"Processors" are businesses, organizations, natural persons or Federal authorities who process personal data on behalf of the controller.

Controllers will continue to be primarily responsible for compliance with the rev-FDPA. Yet, in contrast to the current FDPA, the rev-FDPA will also set out legal obligations applying directly to processors (including data security obligations, restrictions on engaging sub-processors and the requirement to maintain records of processing activities).

The controller-to-processor relationship needs to be governed by a contract (or established by law). The controller needs to be sure that the processor only performs processing activities that the controller would also be allowed to perform, and to ensure that the processor is capable of providing for adequate data security. Further, the rev-FDPA provides that a processor may only hire a sub-processor with the prior consent of the controller. The rev-FDPA will not provide a list of minimum requirements that the contract needs to cover. The standard required by Article 28 of the GDPR will suffice for the purposes of the rev-FDPA.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

In accordance with the key privacy principles (see question 3.3), advertisers need to comply with the following key obligations when collecting, processing, storing or otherwise using personal data as controllers in an advertising context:

(a) Lawfulness: In contrast to EU law, under the (rev-)FDPA, lawfulness of processing does not mean determining a legal basis (eg, legal obligation, contract, legitimate interests or consent) for processing. Rather, it means that businesses or organizations may only process personal data that has been collected in accordance with other applicable laws. For example, processing personal data that has been collected through unlawful trespassing or wiretapping would infringe the lawfulness principle. Legal bases (so-called "justifications") are relevant under the (rev-)FDPA, however, if controllers intend to disclose sensitive personal data to third parties (including disclosure to other group companies), envisage processing for other purposes, or wish to continue processing of personal data despite the data subject's objection.

(b) Fairness: Advisers may only perform such processing activities as data subjects may reasonably expect. Furthermore, fairness means that processing must be performed as described in the privacy policy or other information on data processing provided to the data subjects.

(c) Transparency: Advertisers have to convey to data subjects all information necessary in order to ensure transparent data processing. The information also needs to enable data subjects to exercise their rights under the FDPA. The rev-FDPA will set out in more detail the type of information that controllers need to convey to data subjects. At a minimum, they need to inform data subjects about the identity and contact details of the controller, the contact details of the data protection officer (if any), the purposes of the processing, and (if any) the recipients or categories of recipients of the personal data. Further, if the controller intends to transfer personal data to a recipient in a country which does not offer an adequate level of data protection, the controller also needs to tell data subjects to which countries the controller intends to transfer personal data and based on which safeguards (eg, standard contractual clauses or the Swiss-US Privacy Shield). If the controller has not obtained the personal data directly from the data subject, the controller also needs to inform data subjects about the categories of personal data collected and processed.

Advertisers should provide this information to data subjects in their privacy policy posted on the website and, where appropriate, refer to the privacy policy in marketing material. As regards advertising on publishers' platforms, advertisers should require publishers to provide sufficient notice to their audience as regards their processing of personal data for advertising purposes, including for the use of intermediaries.

(d) Purpose limitation: Advertisers may only process personal data for the specified purposes that have been notified to or are obvious to data subjects; and may only process personal data in a manner compatible with those purposes. Information about the purposes of processing needs to be specific. Advertisers also need to ensure that further processing of personal data received from other controllers is compatible with the purposes determined and communicated at the time of collection.

(e) Proportionality: The processing of personal data needs to be proportionate; that is, limited to what is necessary to achieve the specified purposes, considering the type of personal data concerned and the scope and duration of the processing. The data minimization and storage limitation principles are key aspects of the proportionality principle. This means that advertisers need to limit the scope of data collected and processed to what is necessary for the intended campaigns, and they need to delete personal data once it is no longer needed for advertising or other legitimate purposes (such as compliance with record-keeping obligations).

(f) Accuracy: Advertisers need to ensure they are only processing personal data that is accurate and kept up-to-date. They must take all reasonable steps to ensure that personal data that is inaccurate or incomplete, having regard to the purposes for which it is processed, is deleted or rectified.

(g) Security: Both controllers and (under the rev-FDPA) processors are under an obligation to ensure an adequate level of data security. They need to take technical and organizational measures that are commensurate with the level of risks for data subjects. See question 5.2 for further information on data security requirements under the (rev-)FDPA.

The following are further key or new obligations under the rev-FDPA:

(h) Records of processing activities: Under the rev-FDPA, controllers and processors will (each separately) be required to maintain records of processing activities. Exemptions may apply in relation to low-risk processing of personal data by businesses with less than fifty employees. The Federal Council will draft a revised FDPO once the rev-FDPA is final. This ordinance will lay out the specifics of this and other exemptions that may apply.

(i) Data protection impact assessment: Under the rev-FDPA, controllers will be required to perform DPIAs for intended high-risk processing of personal data. The high risk may result from the type, scope, circumstances or purposes of the processing or from the use of new technologies. A DPIA will be required under the rev-FDPA, in particular, in the case of:

  (i) processing on a large scale of sensitive personal data (see question 3.2), or

  (ii) the systematic monitoring of publicly accessible areas on a large scale.

(j) Representative: Under the rev-FDPA, controllers established outside Switzerland will have to appoint a representative in Switzerland under certain circumstances (see question 2.2).

Appointing a data protection officer ("DPO") is not mandatory for businesses and organizations under the FDPA or the rev-FDPA. But the rev-FDPA incentivizes the appointment of a DPO. For example, with a DPO's involvement in the performance of a DPIA, a controller may avoid having to consult the FDPIC

if the DPIA indicates that the processing would result in a high risk. Businesses which appoint a DPO will have to publish and provide to the FDPIC the contact details of the DPO. It may also be advisable to appoint a DPO voluntarily, as compliance with documentation and notification obligations and responding to data subjects' requests under the (rev-)FDPA require businesses — in practical terms — to establish an internal data protection organization.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Switzerland? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

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 FDPA and the FDPO define a standard for the security of personal data (see question 3.1). Controllers are required to protect the integrity, confidentiality and availability of personal data by means of adequate technical and organizational security measures.

The FDPO sets out a minimum standard: namely, the implemented measures need to protect systems against the risks of unauthorized or accidental deletion, accidental loss, or unauthorized alteration, copying, access to or other unauthorized processing of personal data. The technical and organizational measures need to be adequate to address these risks. The following criteria need to be considered:

(a) the purpose, type and scope of the data processing,

(b) the assessment of potential risks for data subjects, and

(c) the state of the art.

The FDPO sets out types of measures that are considered appropriate, including access control, user logs, encryption, and protection against unauthorized copying, alteration or deletion.

The FDPIC's Guidelines on Technical and Organizational Measures of August 2015 (not available in English) are a useful resource for companies to address this standard and apply the measures set forth in the FDPO. The FDPO will be revised once the rev-FDPA is final.

Under the rev-FDPA, both controllers and processors will be obligated to take technical and organizational measures that are commensurate with the level of risk for data subjects.

6.2 How are data breaches regulated in Switzerland? What are the requirements for responding to data breaches?

The current FDPA does not set out any data breach notification obligations. Under the rev-FDPA, controllers will be required to notify the FDPIC of personal data breaches that may result in a high risk for data subjects. No deadline is defined for the notification. Controllers will need to notify the FDPIC as quickly as possible, ie, 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals have a right to access, rectification or deletion, and to receive a copy of the personal data undergoing processing. They also have a right to object to the processing. After an objection, controllers may only continue processing if they can show that continued processing is necessary in order to comply with a legal obligation laid down in Swiss law, to perform a contract with the data subject or in order to pursue legitimate interests of the controller that are more compelling than the data subject's privacy interests. In addition, individuals have a right to data portability under certain circumstances.

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 in order 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The general framework described above applies to marketing communications, including email, texts, and push notifications. In addition to the data protection requirements set out in the FDPA, 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.

The UCA requires an opt-in in cases where there is no pre-existing business relationship, and requires that businesses offer the recipients an easy way to unsubscribe (opt-out). The Principles of the Swiss Commission for Fairness in Commercial Communication put the statutory requirements concerning marketing communication in more concrete terms. They are also a means to interpret the statutory requirements in an advertising context. For example, continued direct marketing despite an objection by the recipient constitutes aggressive, and hence unfair, advertising according to Principle 4.4.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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.

The rev-FDPA will strengthen the rights of data subjects. The respective information notice obligations of controllers will also apply to the collection of personal data through cookies, pixels and similar technologies. This means that privacy policies also need to address this aspect of data collection. Information (ie, giving notice) is sufficient. No consent requirement applies. Consent may be required where sensitive personal data is disclosed to third parties (including disclosures within a group of companies), in which case consent has to be explicit.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

The general framework described above applies to the processing of personal data in connection with targeted advertising and behavioral advertising. The obligations of the rev-FDPA concerning profiling require special attention. Explicit consent may be required before using profiling in the context of targeted advertising, particularly where (sensitive) personal data is disclosed to third parties or where many data subjects are likely to object to processing by means of profiling. However, this point will remain unclear until the Federal Parliament has reached an agreement on a final text of the rev-FDPA.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The general framework described above applies to the processing of personal data in connection with customer matching. Advertisers who use Facebook Custom Audiences or LiveRamp need to ensure their continued processing for advertising purposes is compatible with the purposes specified at the time of collection. Advertisers may be considered joint controllers (together with Facebook) in relation to data collection in the context of Custom Audiences (applicable in Switzerland if the FDPIC and the courts follow the practice developed under the EU GDPR). In that case, they are responsible — jointly with the customer-matching provider — for providing sufficient notice and, where applicable, requesting consents.

Typically, advertisers will rely on notices provided and, where applicable, consents requested by the providers of customer matching services (eg, Facebook). Yet there is a risk that the FDPIC or courts may deem the information and consent provided by the respective service provider to be insufficient. Advertisers should, at least, explain in general terms (eg, in their website privacy policy) if they use customer matching or similar marketing technologies to target potential customers.

8.5 Are there specific privacy rules governing data brokers?

There are no specific privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

The general framework described above applies to the processing of personal data in social media. Advertisers should inform data subjects in their website privacy policies about their social media marketing activities.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

The general framework described above applies to the processing of personal data in connection with loyalty programs and promotions. The provisions of the (rev-)FDPA concerning profiling require special attention. Also, the FDPIC has in the past closely scrutinized the information provided in privacy policies concerning loyalty programs.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Under the current FDPA, the FDPIC publishes a list of states that, according to the FDPIC's assessment, provide an adequate level of data protection. Under the rev-FDPA, the Federal Council will adopt adequacy decisions in relation to jurisdictions that provide an adequate level of protection. The Federal Council will (just as the FDPIC has done in the past) likely follow the European Commission's lead, and consider adequate those jurisdictions in relation to which the European Commission has adopted an adequacy decision.

Appropriate safeguards are required in order to transfer personal data to states without an adequate level of protection. Appropriate safeguards include, under the (rev-)FDPA:

(a) standard contractual clauses issued, approved or recognized by the FDPIC;

(b) binding corporate rules approved by the FDPIC or a competent data protection supervisory authority in a state that provides adequate protection;

(c) (subject to prior notification to the FDPIC) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data abroad; and

(d) international treaties to which Switzerland is a party may serve as appropriate safeguard.

The same safeguards may be used for cross-border transfers within a group of companies.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

For the purposes of the (rev-)FDPA, companies within a group of companies are considered as third parties. Hence, a transfer to another company within a group of company constitutes a disclosure to a third party.

Companies within a group of companies need to ensure they adhere to the principle of purpose limitation and to notification obligations, if further processing data they receive from other group companies. Special justification (eg, explicit consent or overriding legitimate interests) is required for the disclosure — including within a group of companies — of sensitive personal data. 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).

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The FDPIC does not (and will not under the rev-FDPA) have the right to issue administrative fines. The state prosecutors enforce the criminal law provisions of the FDPA.

Currently, the FDPA provides that private individuals may be fined up to CHF 10,000 if they are responsible for the violation of specific information and notification requirements under the FDPA (eg, willfully providing false or incomplete information in response to a data subject access request).

Under the rev-FDPA, the maximum amount of the fine will be CHF 250,000. The rev-FDPA will also extend criminal liability to the violation of additional data protection obligations under the rev-FDPA, such as failing to ensure there are sufficient guarantees for international data transfers, or failure to comply with minimum data security requirements.

The rev-FDPA will also introduce criminal liability of businesses and organizations. The responsible individuals (eg, directors or managers) will primarily be liable. However, the business or organization (controller or processor) may be held liable for a fine of up to CHF 50,000 under the rev-FDPA if determining who, in the organization, is responsible for the infringement would require disproportionate investigative efforts.

10.2 Do individuals have a private right of action? What are the potential remedies?

Article 28 of the CC provides for private rights of action against infringements of personality rights. The following remedies are available:

(a) prior restraints and other pre-publication injunctions,

(b) removal of an existing infringement (this may include a right to be forgotten),

(c) a declaratory judgment (if the effect of the infringement is continuing), and

(d) claims for compensatory damages, moral damages, and disgorgement of profits (Article 28a of the CC).

The FDPA provides private rights of actions against infringements of personality rights protected under the FDPA. 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 Article 28a of the CC apply by analogy to such claims brought under Article 15 of the FDPA. This will remain unchanged under the rev-FDPA.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Switzerland which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The FDPA is under revision. Advertisers should particularly review the requirements concerning profiling once an agreement on the final text of the rev-FDPA has been reached. 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 cautions around processing personal information/personal data in Switzerland?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/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 create 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.

12.2 What do you envision the privacy landscape will look like in 5 years?

On the legislative landscape, the completion of the revision of the FDPA will likely further increase awareness 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.

Still, internal and external resources for privacy compliance are not yet a given. Companies with data-driven business models and companies and organizations in highly regulated sectors will likely be among those who adapt their data processing activities in the wake of regulatory changes.

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 will much depend on the resources made available to the FDPIC, which have so far been rather limited. The rev-FDPA will empower 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 rev-FDPA, therefore, may remain rather limited too.

12.3 What are some of the 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 12.2) 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. 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.

TURKEY

1 PRIVACY LAW

1.1 How is privacy regulated in Turkey?

Article 20 of 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 Turkish Penal Code also includes some provisions related to crimes concerning personal data.

The DPL is modelled on the 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. The DPL also adopted certain concepts from the GDPR, such as data breach notification, however, it is more similar to the EU Directive than to the GDPR.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

As mentioned above, the main legislation governing privacy in Turkey is the DPL. The Turkish Penal Code also includes some provisions, criminalizing certain activities such as 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 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

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. If there is non-compliance, the Board can request that the data controller or data processor comply with DPL. Additionally, the Board has been given the authority to impose administrative fines on data controllers for breaches of the DPL.

In addition to administrative fines, non-compliance with the provisions related to personal data can result in criminal sanctions (see question 10.1).

Since its establishment in January 2017, the Board has followed up and investigated violations of the DPL and its secondary legislation, and has rendered several decisions where it has imposed administrative fines.

2 SCOPE

2.1 Which companies are 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 companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

There is no specific territoriality provision under the DPL. However, by consideration of Article 1 of the DPL, which states that the 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.

Data controllers located abroad are under an obligation 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 INFORMATION

3.1 How is personal information/personal data defined in Turkey?

Under the DPL, "personal data" is defined as "any information relating to an identified or identifiable natural person."

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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.

Processing sensitive personal data is subject to stricter conditions than processing non-sensitive personal data. Other than personal data relating to health and sexual life, such data may only be processed either on the basis of explicit consent or where processing is expressly permitted by law.

Personal data relating to a person's health and sexual life may only be processed by persons under the obligation of secrecy or authorized institutions and organizations, and on the basis of the explicit consent of the data subject, or for the purposes of:

(a) protection of public health,

(b) operation of preventive medicine,

(c) medical diagnosis, treatment, and care services, or

(d) planning/management of health services and its financing.

Moreover, in addition to the above, the DPL provides that, as an additional condition, sufficient measures determined by the Board must be adopted for the processing of sensitive personal data. The Board has published the "Decision regarding the Adequate Measures to be taken by Data Controllers in Processing of Personal Data of Sensitive Nature", under which it has determined the technical and administrative measures to be taken by data controllers who process sensitive personal data.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The principles to be complied with when processing personal data are:

(a) being in conformity with the law and good faith;

(b) being accurate and, if necessary, up to date;

(c) being processed for specified, explicit, and legitimate purposes;

(d) being relevant, limited and proportionate to the purposes for which the data is processed; and

(e) being stored only for the time designated by relevant legislation or necessitated by the purpose for which data are collected.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

Yes, the DPL assigns two different roles to companies, based on how they process personal data. A company or an individual can be a data controller or a data processor:

(a) Data Controller: This is a natural or legal person which determines the purposes and means of the processing of personal data, and which is responsible for the establishment and management of the data filing system. The data controller is the main responsible party with regard to data processing.

(b) Data Processor: This is a natural or legal person who processes personal data based on the authority granted by and on behalf of the data controller.

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, it will always be the data controller which will be the main responsible party vis-à-vis the DPA.

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. The Board has also published sample undertakings to be signed between data controllers and data processors. The Board published those undertakings not as a mandatory general form to be used in all transactions between data controllers and data processors, but only for cases where a data transfer will be made outside Turkey. However, these samples 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.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Personal data must be processed on the basis of one of the legal grounds set out in the DPL and in accordance with the principles set forth under the DPL (see question 3.3).

Another important obligation concerns informing data subjects. Before processing personal data, data controllers must inform the data subjects of the following issues with a privacy notice:

(a) the identity of the data controller and its representative (if the data controller is located abroad);

(b) the purposes for which personal data will be processed;

(c) the persons to whom personal data might be transferred and the purposes for the same;

(d) the method and legal basis of collection of data; and

(e) the rights of data subjects set forth under the DPL.

Data controllers located abroad must appoint a representative, which 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.

Data controllers must register themselves 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:

(a) categories of personal data processed by the data controller;

(a) the purposes of processing of each personal data category;

(b) data subject groups;

(c) groups of recipients of personal data;

(d) whether or not the relevant personal data category is transferred abroad;

(e) measures taken for the security of personal data; and

(f) the maximum period of retention.

Regarding data security, by Article 12 of the DPL, 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Turkey? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The main obligation related to data security for personal data is set forth under Article 12 of the DPL (see question 5.1).

The DPA has published guidelines to explain what kind of security measures a data controller should take. The guidelines provide examples of:

(a) administrative security measures, such as training employees, minimizing personal data, managing the relationship with data processors; and

(b) technical measures, such as ensuring cyber security and managing security in the cloud.

6.2 How are data breaches regulated in Turkey? What are the requirements for responding to data breaches?

Under the DPL, in case of data breach, the data controller must notify the data subject and the Board of such situation as soon as possible. The Board has issued a decision stating that the term "as soon as possible" shall be interpreted as "within 72 hours of the time the data controller becomes aware of the breach".

In terms of the notification obligation, there is an important difference between the DPL and the EU's GDPR — the obligation to notify the breach under the DPL is a very straightforward obligation; no analysis needs to be made about the effect of the breach on the rights and freedom of the data subjects. If there is a breach, that breach must be notified both to the Board and the data subjects.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Everyone, by applying to the data controller, has the right to:

(a) learn whether or not her/his personal data has been processed;

(b) request information as to processing, if her/his 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 personal data has been transferred;

(e) request rectification in cases where personal data has been processed incompletely or inaccurately;

(f) request deletion or destruction of 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 occurrence of any result that is to her/his detriment by means of analysis of personal data exclusively through automated systems; and

(i) request compensation in cases where he/she incurs damage due to the unlawful processing of his/her personal data.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

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.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

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.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Under Turkish Law, there is no provision specific to targeted/behavioral advertising. As a personal data processing activity, targeted/behavioral advertising is subject to the principles and procedures set forth under the DPL. Under the general provisions of the DPL, targeted/behavioral advertising activities would be subject to the consent of the data subject, as they include an element of profiling, which cannot be covered by the legitimate interest of the data controllers involved in those activities.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

In the privacy notices they send to their customers, advertisers need to include information on:

(a) the third parties (as a category) with whom they share personal data; and

(b) why they are sharing that data (ie, so that targeted advertising can be made).

In addition to the privacy notice, the advertisers need to obtain the explicit consent of their customers in order to share such data with those third parties.

8.5 Are there specific privacy rules governing data brokers?

No, under Turkish Law, there are no specific rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

From a privacy perspective, social media is regulated under the general provisions of the DPL. In addition, Law No 5651 on the Prevention on Crimes Committed through the Internet provides that an individual can request the removal of content if such content violates her/his privacy.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Under Turkish Law, there is no provision specific to loyalty programs and promotions from a privacy perspective. Therefore, 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 to participants. The existence of choice, stated the Board, is an indicator that participants willingly gave their consent for processing.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Personal data can be transferred to a third party located inside Turkey if the data subject gives her/his explicit consent, or if there is another legal ground for such transfer set forth under the DPL.

In order to transfer personal data outside Turkey (either to a third party located abroad or to a server located abroad, even if it is owned by the transferring data controller), either:

(a) the explicit consent of the data subject must be obtained; or

(b) one of the additional legal grounds of data processing set forth under the DPL must apply to the transfer and:

  (i) the destination country must be one of the countries providing adequate protection; such countries will be determined by the Board; or

  (ii) if the destination country does not provide adequate protection, both of the following conditions should be met:

(1) the data controller in Turkey and in the foreign country must provide a written commitment, stating that sufficient data protection will be provided; and

(2) the transfer must be authorized by the Board.

The Board has yet to issue a list of countries providing adequate protection. Thus, transfer of personal data can be made only with the explicit consent of the data subject or with the permission of the Board as mentioned under (b)(ii)(2) above.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Currently, there is no regulation for transfer of data between group companies. However, the DPA and the Board are preparing to publish a set of rules to govern the transfer of personal data between group companies, which is expected to be similar to the Binding Corporate Rules mechanism under the GDPR.

One point to consider is that the DPL does not provide a definition for a "third party"; therefore, any individual or entity (other than the data controller and the data subject) can be considered a third party. This creates a problem in relation to transfers between data controllers and data processors, as any transfer of personal data from a data controller to a data processor can be interpreted as a transfer to a third party. Such an interpretation would mean that the transfer should be based on one of the legal grounds in the DPL. It is possible to think that in most cases, such a transfer would fall under the scope of the legal ground of legitimate interest. However, such an approach would require a separate analysis for each transfer.

A different approach is possible, whereby the solution to the problem mentioned above would lie with the interpretation of the definition of "data processor" under the DPL. As the data processor is an individual or a legal entity processing personal data "on behalf of" the data controller, it could be argued that the data processor is not an ordinary third party. It acts under the authority of the data controller, making the data processor a part of the data controller's organization. As the transfer of personal data between employees of a data controller cannot be considered a transfer to a third party (although the data controller and each employee is a separate entity), it might be possible to state that the transfer to a data processor should not be considered as a transfer to a third party. This is a tenuous interpretation but if the Board adopts a decision in this respect, such an interpretation would get stronger and its chances of holding out against the test of a court would be higher.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

(a) Administrative fines (NB amounts are as at November 2019):

(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 7,352 and TRY 147,058. (approx US $1,280–25,600).

(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 22,057 and TRY 1,470,580 (approx US $3,840–255,640).

(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 36,763 and TRY 1,470,580 (approx US $6,400–255,640).

(iv) If the data controller does not register itself with the Data Controllers' Registry, it will be subject to an administrative fine between TRY 29,410 and TRY 1,470,580 (approx US $5,110–255,640).

(b) Criminal sanctions:

(i) for unlawfully recording the personal data of another, imprisonment of between one and three years;

(ii) for unlawfully transferring/acquiring another person's personal data to/from another person, imprisonment between two and four years,

(iii) for not anonymizing, deleting or destroying personal data after the legally permitted period, imprisonment between one and two years.

10.2 Do individuals have a private right of action? What are the potential remedies?

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 Board would order the cessation of such activity.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Turkey which affect privacy?

The concept of privacy, in the sense that it is used in the European Union, is relatively new to Turkey, because the DPL is the first general legal framework for privacy, and it only came into force in 2016. Before then, most data controllers did not have any notion about privacy, and they are slowly coming to terms with what is required of them in relation to privacy issues. One of the results of this is that the level of compliance differs dramatically among data controllers in Turkey.

The DPL also had an effect on data subjects; they are becoming more and more aware of their privacy rights, and the number of complaints made to the Board rises each day. However, the depth of knowledge of data subjects about privacy is still not high, and sometimes privacy notices may create doubts in the minds of data subjects instead of eliminating them. The fact that a data controller is handling their data, however proper such handling may be, and informing them of such processing activity, may create suspicions of wrongdoing on the part of some data subjects. Therefore, the wording of privacy notices must be prepared very carefully in order to prevent such doubts and eliminate the risk of complaints to the Board.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

There are discussions on amending some of the provisions of the DPL which have been found to be problematic. There is no clear timeline as to when such amendments would be made.

A list of countries providing adequate protection is also a matter that has long been awaited by data controllers. However, it still not clear when, or even whether, such a list will be published.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Turkey?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Until recently, there was no general privacy legislation; there were only a few provisions of the Turkish Criminal Code related to personal data, and not many court decisions had been made on those provisions. There had been various drafts of a general privacy legislation in the past, but none of them had entered into force before the DPL. A general legislation regarding data protection was one of the conditions for lifting the visa requirement between the European Union and Turkey, and this was the main motivation behind the enactment of the DPL. Be that as it may, the DPL has brought about significant changes in Turkish data privacy landscape. Especially since, after the DPA was established and the Board was elected, various guidelines and secondary legislation were prepared. The fact that the DPA and the Board took their jobs seriously also affected the players in the market, and the DPL became one of the important pieces of legislation in the Turkish legal framework.

12.2 What do you envision the privacy landscape will look like in 5 years?

Both data controllers and data subjects, and also the DPA and the Board, will have far more experience with the different concepts of privacy in five years' time, as these concepts will not be new by then. In five years, the level of compliance among data controllers will rise, and the level of awareness of data subjects will increase in parallel with that rise. Consequentially, the expertise of the DPA and the Board will reach higher levels. We will see more complicated cases handled by the Board, which will lead to more detailed and sophisticated decisions.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The DPL is a law modelled on the Data Protection Directive (95/46/EC). When such Directive came into force, the internet was not such a big part of daily life, and the amount of data collected by data controllers was not as huge as it is now. Therefore, companies in the European Union had time to adapt their privacy practice to developments in the technology. However, the DPL came into force in 2016, a time when companies had already been used to collecting and processing high amounts of data with various processing activities. It has therefore been more difficult for Turkish companies to review all of their previous practices and make the adaptations required by the DPL.

UKRAINE

1 PRIVACY LAW

1.1 How is privacy regulated in Ukraine?

The current Ukrainian legislation is mainly based on the old Data Protection Directive (95/46/EC), with the addition of certain specifics (eg, concerning the Ukrainian data protection authority).

Led by the commitments in the Association Agreement with the EU, in October 2017, the Ukrainian Parliament planned to implement the regulations of the EU General Data Protection Regulation ("GDPR") into national legislation by 25 May 2018. However, this goal has still not been achieved. There have been several unsuccessful attempts to draft an implementation bill. However, such implementation is expected to be conducted by the newly elected Parliament.

The legal enforcement of data privacy rights in Ukraine is still not as strong as, eg, 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 increases within certain industry sectors (eg, IT and telecommunications), Ukrainian business is quite reluctant to implement self-regulating mechanisms.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The Constitution of Ukraine dated 28 June 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 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981.

However, these do not 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 Law of Ukraine On Telecommunications dated November 18, 2003, and the Law of Ukraine On Electronic Commerce). These laws contain some limited regulation on privacy for certain types of marketing activities (eg, email marketing).

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The central competent Data Privacy Authority of Ukraine 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 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 as it is limited by respective laws.

A violation of the Ukrainian privacy laws may also result in civil or even criminal liability (in very rare cases related to illegal collection and distribution of personal data).

There are several other state bodies which have limited privacy enforcement powers in certain industries (eg, the telecoms regulator, consumer protection authority).

As yet, there is no known enforcement practice originated by self-regulatory bodies in Ukraine.

2 SCOPE

2.1 Which companies are 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.

2.2 Does privacy law in Ukraine apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

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 to 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.

There are no specific obligations relating to companies outside Ukraine other than the necessity to notify the Ombudsman on the processing of so-called "extreme risks personal data" (see, further, question 3.2) to the extent that such processing affects Ukraine in any way.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The Privacy Act names the following types of personal data to be sensitive:

(a) race, ethnic origin and nationality;

(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) any pre-trial procedures;

(j) any investigative procedures against him/her;

(k) violence against him/her; and

(l) location and travel routes.

The specific obligations regarding the processing of extreme risks personal data involve filing appropriate notifications to the Ombudsman. 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, including any data breach notifications and cross-border data transfer. Once extreme risk personal data is processed, it is also necessary to notify the Ombudsman of a data processing division or the appointment of a data protection officer. Such notification can be filed simultaneously with the notification of extreme risk personal data processing. The foregoing local notifications are not required if processing the extreme risk personal data falls within the statutory exemptions (eg, it is processed the purpose of execution of controller's rights and fulfilment of the controller's obligations within employment relations).

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The privacy laws in Ukraine do not contain dedicated provisions naming 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 — meaning that personal data must be processed lawfully, fairly and in a transparent manner;

(b) lawful basis for processing — meaning that personal data may be only processed if it falls within the grounds for processing envisaged by the Ukrainian laws;

(c) purpose limitation — that processing of personal data be carried out only for specified, explicit and legitimate purpose known to the data subject;

(d) data minimization — personal data must be adequate, relevant and limited to what is necessary in relation to the purpose of the processing;

(e) retention (storage limitation) —the 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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

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. Additionally, 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 the 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 include a data processor in the processing activities. However, Ukrainian law foresees a written agreement between the controller and the processor. Unlike the GDPR, Ukrainian law does not prescribe minimum content and requirements concerning this agreement (in contrast, eg, to Article 28 of the GDPR).

Under the Privacy Act, the obligations of controllers and processors in terms of processing activities are almost the same, apart from some specific obligations, which include notification requirements for controllers or compliance with controller's instructions for processors.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

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 — a legal requirement to notify the data subject in relation to personal data collection on the day of the collection (if collected from data subject) or within 30 business days after such 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 — a legal requirement for the controllers and processors to undertake adequate security measures as regards processed personal data.

(c) Recording requirements — a requirement for the 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) view of personal data;

(iv) any transfer (copying) of personal data of a data subject;

(v) date and time of personal data deletion or erasing;

(vi) a person who made any of the above actions; and

(vii) purpose and reasons for alternation, view, transfer and deletion or erasure of personal data.

The described information shall be stored by the data controller/processor for one year, beginning at the end of the year in which the processing of personal data took place, unless otherwise stipulated by the applicable Ukrainian laws.

The Master Template is generally considered as not 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.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Ukraine? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

As of now, there are 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.

6.2 How are data breaches regulated in Ukraine? What are the requirements for responding to data breaches?

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, although there are no legal requirements for data breach notifications, 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.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Under Article 8 of the Privacy Act, data subjects have the following rights in Ukraine:

(a) to know about the sources of collection, the location of their personal data, the purpose of the processing, the location or place of residence of the controller or processor of the personal data, or to give appropriate instructions for receiving this information by their authorized persons, or as otherwise provided by law;

(b) to receive information about the conditions of access to personal data, including information about third parties to whom his/her personal data is transferred;

(c) to access his/her personal data;

(d) unless otherwise provided by law, to receive within thirty calendar days from the date of receipt of the request, a reply on whether his/her personal data is being processed, and to receive the contents of such personal data;

(e) to submit a reasonable request to a controller with an objection to the processing his/her personal data;

(f) to submit a reasonable request to change or destroy his/her personal data held by any controller and processor, if such data is processed illegally or is unreliable;

(g) to protect his/her personal data from unauthorized processing and accidental loss, destruction, damage due to intentional concealment, failure to provide or untimely disclosure, as well as to protect it against the provision of information that is inaccurate or detrimental to the honor, dignity and goodwill of an individual;

(h) to submit complaints about the processing of personal data to the authority or to court;

(i) to use remedies in case of violation of the laws on personal data protection;

(j) when giving consent, to make reservations restricting the right to process his/her personal data;

(k) to withdraw consent to the processing of his/her personal data;

(l) to be informed about any form of automated processing of his/her personal data; and

(m) to enjoy protection against any automated decision that may have legal implications for him/her.

Although the above rights are quite exhaustive, current case law in Ukraine suggests that the appetite is quite low for Ukrainian data subjects to defend their rights before the applicable authorities and courts.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Ukrainian law does not define or regulate in detail the marketing communications. The following general rules may apply:

(a) Law of Ukraine On Electronic Commerce (the "E-commerce Law")

The E-commerce Law defines "commercial electronic messages" (solicitation letters) as electronic messages in any form which purpose is direct or indirect promotion of goods, work or services or business reputation of a person which conduct commercial or independent professional activity.

Commercial electronic messages may be sent to an addressee (eg, potential buyer) only with his/her express consent, unless the addressee has the opportunity to unsubscribe from further receiving such messages.

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 the recipients with direct and easy access to the 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 shall be available and worded in a way to avoid ambiguity as well as comply with the 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, information on delivery costs.

The E-Commerce Law expressly prohibits the practice whereby the fact of receipt of the advertising message by the consumer without his/her 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) Law of Ukraine On Advertising ("Advertising Act")

The Advertising Act establishes specific requirements regarding the promotion of services via the 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) Code of Mobile Marketing

The main mobile operators and market players in the Ukrainian market have adopted the Code of Mobile Marketing (as a non-binding soft law), which sets out principles, conditions and procedures of mobile marketing (via SMS and MMS). Specifically, the Code sets out the requirements with respect to consumer choice and registration, consumer-related communication, termination of participation in a marketing event, as well as limitations of activities.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Ukrainian law does not regulate the use of tracking technologies.

Under the general rules (see question 8.1(a)), commercial electronic messages must be sent to the addressee (eg, potential buyer) only with his/her express consent, unless the addressee has the opportunity to unsubscribe from further receiving such messages.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Ukraine does not have dedicated rules addressing targeted advertising and behavioral advertising. Rather, the general rules outlined above (see question 8.1(a)) apply.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Ukrainian law does not directly regulate issues on sharing personal data with third parties for customer matching.

The Privacy Act provides for general rules obligatory for each data controller. Thus, if the advertiser acts as a data controller, prior explicit consent on the collection and further processing of personal data is generally required. Such consent should include permission to transfer the person's personal data to third parties. Furthermore, where, notification of transfer is required under the data subject's consent, the Privacy Act requires the data controller to notify a person as to the fact of the transfer of his/her personal data within 10 days.

8.5 Are there specific privacy rules governing data brokers?

Ukrainian law does not regulate activities of data brokers. General rules and regulations apply.

It should be noted that Ukrainian law limits certain activities with personal data. In particular, breach of privacy (namely the illegal collection, storage, use, removal, distribution of confidential information about a person or illegal alteration of such information) is subject to criminal liability (Article 182 of the Criminal Code of Ukraine). Illegal disposal or distribution of information with limited access (in particular, which is stored on computers, automated systems, and computer networks or data storage devices) is also subject to criminal liability (Article 361-2 of the Criminal Code of Ukraine).

8.6 How is social media regulated from a privacy perspective?

Ukrainian law does not regulate this issue.

Under the general rules, advertising on the Internet, including in social media, is regulated in the same manner as offline advertising. Statutory regulation comprises specific advertising-related laws and general legislation. From a practical interpretation, marketing/advertising in social media should be in line with the Advertising Act if:

(a) the social media is located within a Ukrainian segment of the Internet (eg, registered in domain .UA);

(b) customers targeted by such advertising are located in the territory of Ukraine; or

(c) advertising is placed by technical means located in the territory of Ukraine.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

If the data subject's personal data is collected and processed as a condition to participate in a loyalty program/promotion, its official terms must contain provisions relating to obtaining explicit consent from the data subject (it must set out, among other matters, the specific purpose of the personal data processing and the scope of the processed personal data).

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

According to Article 29 of the Privacy Act, cross-border data transfers are allowed to countries that provide an adequate protection of personal data. Members of the EU and 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. Moreover, the Article provides that the Cabinet of Ministers of Ukraine (Ukrainian government) will adopt a list of countries that provide an adequate level of personal data protection (though no such list has yet been adopted).

Cross-border transfers of personal data are allowed from Ukraine under one of the following bases:

(a) an express consent to cross-border transfer;

(b) it is necessary to conclude or perform a transaction between the data controller and a third party for the benefit of the data subject;

(c) it is necessary to protect the vital interests of data subjects;

(d) it 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.]

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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.

In April 2013, the Working Group on Personal Data Protection at the American Chamber of Commerce in Ukraine prepared the Template Data Transfer Agreements ("AmCham Template"). Whilst these 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 are developing their agreements using either the AmCham Template or the standard (model) contractual clauses, which were adopted by the European Commission.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

The Ombudsman, courts and police are responsible for enforcing the requirements of the Privacy Act. According to the legislation, it 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 for an administrative penalty, where the highest fine can be the equivalent of about EUR 1,000. There is a risk of criminal liability (with a worst-case scenario of either corrective labor up to 2 years or with arrest for up to 6 months or with personal restraint for up to 3 years), but the enforcement practice to date is 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.

The appetite of data subjects for filing a court claim for compensatory damages in Ukraine is also very low.

The risk of being fined by the Ombudsman is also currently low.

10.2 Do individuals have a private right of action? What are the potential remedies?

Under Ukrainian legislation, individuals have a private right of action. Individuals in Ukraine can apply to the Ombudsman, police or to the courts to seek legal protection for any illegal processing of their personal data. Moreover, in accordance with Article 8 of 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.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Ukraine which affect privacy?

There are no special cultural features regarding privacy in Ukraine. Generally speaking, Ukrainian citizens are not very familiar with their rights regarding privacy and personal data. Because the laws of Ukraine do not impose any substantial fines or liability for data breaches or other privacy-related infringements, businesses implement only the minimum requirements established by the Privacy Act. Moreover, the enforcement practice to date is minimal and does not explicitly relate to international business.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

Led by the commitments in the Association Agreement with the EU in October 2017, the Ukrainian Parliament planned to implement the GDPR into national legislation by May 25, 2018. However, this goal has not yet been met. There have been several unsuccessful attempts to draft an implementation bill, and new GDPR implementation bills are expected from the newly elected Parliament. In addition to the GDPR, the Ukrainian Parliament has planned to implement the e-Privacy Directive as a part of the process of integrating EU and Ukrainian legislation.

In 2018, the Ukrainian data protection authority finished collaborating on the project, the EU Twinning Ombudsman, which was supported by a team of Lithuanian and Austrian partners. The EU Twinning Ombudsman has drafted a new draft law of Ukraine "On Protection of Personal Data." However, the Ukrainian Parliament has not yet addressed the draft law. On November 12, 2019, the Ombudsman established an interagency working group on the development of legislative proposals in the field of personal data protection, which will finalize the work of EU Twinning Ombudsman and address the draft law to the Ukrainian Parliament. With the election of a new President and the Parliamentary elections held in 2019, this matter is likely to be reviewed by a new presidential administration, government and parliament. Currently, the position of the newly elected President on this matter is unclear. Therefore, it is advisable to monitor this issue over the coming year.

One of the much-anticipated developments in the privacy landscape in Ukraine relates to the Ukrainian IT associations' application to the EU Commission for an adequacy decision under Article 45 of the GDPR for the Ukrainian IT industry as a 'specified sector within third country'.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Ukraine?

The Ombudsman and the Department of Personal Data (a special division within the Ombudsman's office) are responsible for implementing the Ombudsman's powers relating to personal data protection and have several additional responsibilities, namely:

(a) monitoring compliance with the existing data protection laws and regulations;

(b) preparation of regulatory changes, bills, and proposals for prevention of personal data violations;

(c) conducting scheduled and unscheduled inspections (according to the information on the Ombudsman's website, the last inspection took place in May 2019); and

(d) keeping a search base of personal data controllers.

All other duties of the Ombudsman can be found on the Ombudsman's website.

However, despite there being a long list of official duties of the Ombudsman, his activity in the field of personal data is quite weak. At the same time, the Ombudsman has been quite efficient at interpreting laws. For example, the Ombudsman has developed several guidelines, which are very important for business and bring clarity for some data-related issues. In particular, the following guidelines have been approved by the Ombudsman:

- Model Rules on Personal Data Processing;
- Rules on Exercising Control by the Ukrainian Parliament Commissioner for Human Rights over Compliance with Laws on Personal Data Protection; and
- The Procedure of Notification of the Ukrainian Parliament's Commissioner for Human Rights on the Processing of Personal Data, which is of Particular Risk to the Rights and Freedoms of Personal Data Subjects, on the Structural Unit or Responsible Person that Organizes the Work Related to Protection of Personal Data during Processing Thereof.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Since the Privacy Act entered into force in 2011, there have been only two significant changes in the sphere of privacy or personal data protection. From January 1, 2014, all functions relating to the protection of personal data in Ukraine were transferred from the State Service of Personal Data Protection to the Ombudsman; and the requirement to register databases that contain personal data was cancelled. Since that time, data controllers are obliged to notify the Ombudsman whenever they process data that is categorized as extreme risks personal data.

12.2 What do you envision the privacy landscape will look like in 5 years?

As Ukraine is a prospective member of the European Union, it is obliged to harmonize its legislation with the standards of EU legislation. Therefore, we assume that both the GDPR, the e-Privacy Directive, and other privacy-related legislation will be adopted by the Ukrainian Government. Based on the continuous adaptation of Ukrainian legislation to EU standards, it is likely that the GDPR will be adopted within the next four years.

Basing 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.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

For now, there are no major privacy related challenges for companies who are doing business in Ukraine. The main challenges as of now are data protection rules for processing and transferring sensitive/extreme risks personal data both in and outside Ukraine.

As no relevant changes have been made since 2014, there are no new challenges for the companies. 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.

UNITED ARAB EMIRATES

1 PRIVACY LAW

1.1 How is privacy regulated in United Arab Emirates?

Currently, there are no general data protection laws in the UAE, nor are there explicit laws or authorities that deal specifically with privacy in the UAE (other than in the Dubai International Financial Centre ("DIFC") and Abu Dhabi Global Market ("ADGM") Free Zones). However, there is an expectation that such laws will be passed in the near future, reflecting the global interest in this area of law.

However, there are a number of UAE Laws and legal provisions of general application in the context privacy and data protection that can be considered to be relevant to protecting data subjects against unauthorized disclosure of personal data. These provide for both criminal and civil sanctions against unauthorized disclosure of personal data.

While these types of provisions are not entirely consistent with the approach to data privacy issues addressed in modern data protection laws in other jurisdictions, nor as extensive, they must still be considered when assessing the legal basis for processing personal data in the UAE, and associated transfers of personal data to recipients outside the UAE.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

While the UAE does not have comprehensive data protection legislation in the style of the California Consumer Privacy Act ("CCPA") or General Data Protection Regulation ("GDPR") (other than in a few free zones, including, most notably, the DIFC and ADGM), there are provisions of general application in relation to the processing, transfer and disclosure of personal data or confidential information. The key laws are the following:

(a) The UAE Constitution: Article 31 is considered to grant a general right to privacy for citizens of the UAE, as it provides for the right to freedom and secrecy of communication by post, telegraph or other means of communication under law.

(b) Federal Law No 3 of 1987 ("Penal Code"): Article 379 imposes sanctions on:

> "Any individual who, by reason of his profession, craft, circumstance or art is entrusted with a secret and who discloses it in cases other than those permitted by the law, or who uses it for his own advantage or another person's advantage ... unless the individual to whom the secret pertains has consented that it be disclosed or used."

While there is no guidance in relation to the definition of "secret", personal data would certainly be capable of being considered a "secret", depending, of course, on the nature of the data and the manner in which it was revealed.

In addition, Article 380 (bis) adds:

> "Detention shall be inflicted upon whoever unrightfully copies, distributes or provides another person with the content of a phone call or message or information or data or any other such things that he examines by virtue of his profession".

(c) Federal Law No 5 of 2012 relating to Combating Information Technology Crimes ("Cyber Crimes Law") also contains provisions that are relevant to the area; imposing sanctions on gaining access to a website, IT system or computer network without (or in excess of) authorization, with increased sanctions where the access results in(amongst other things) disclosure of any data or information, especially where the information is personal information. Note that it imposes the liability on the perpetrator — there is no obligation on the entity holding the data to act in a particular manner. The unauthorized use of any IT system to disclose confidential information obtained during the course of employment is also sanctioned (see, further, question 10.1).

While these types of provisions differ from the approach to data protection issues in other jurisdictions, they should be considered when assessing the legal basis for processing personal information in the UAE, and associated transfers of personal data to recipients outside the UAE. Ultimately, the risk under UAE law tends to be managed by way of suitable consent from the data subject, despite it being clear that specific written consent is not a strict legal requirement in all circumstances.

In addition, a variety of laws relating to the protection of data that is held in relation to health insurance, patient confidentiality, and creditworthiness contain specific provisions related to privacy and data protection.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Outside of the free zones noted above, where provisions will apply only to companies that are established in those free zones, there is no regulatory authority specifically addressing privacy in the UAE. There are also no self-regulatory bodies. Breach of the Penal Code or Cyber Crimes Law will give rise to criminal liability (and hence a police prosecution). It would also (alternatively, or in addition) allow for civil recovery of damages under Federal Law No 5 of 1985 on the Civil Transactions Law of the United Arab Emirates ("Civil Code"). The Civil Code does not specifically refer to the disclosure of data or confidential information, but its terms in relation to recovery of damages for acts caused by a third person could be applied in that manner.

2 SCOPE

2.1 Which companies are subject to privacy law in United Arab Emirates?

Because the law is a general law that protects data in a very general manner, it can apply to all companies that operate in the UAE.

2.2 Does privacy law in United Arab Emirates apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The criminal laws (Penal Code and the Cyber Crimes Law) will be difficult to enforce against an entity ex-territorially and, indeed, the Cyber Crimes Law in particular has a provision that notes that, in respect of a crime that takes place outside of the UAE, it will only have jurisdiction if the target was a UAE government entity.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in United Arab Emirates?

There is no definition of "personal data". The laws variously use the terms "secret information" "private" matters and the like. There is no guidance as to whether the use of the different terms was intentional, or whether they are meant to signify different types of information or data.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Outside of the specific regulations in relation to health insurance, patient confidentiality, and creditworthiness, there are no categories listed.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The law does not include principles such as these. The most important aspect for each of the laws listed above would be the obtaining of consent from the data subject.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

These roles are not expressly assigned under any UAE law.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

These key obligations are not specify required under any UAE law.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in United Arab Emirates? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

This is not specifically covered under any UAE law.

6.2 How are data breaches regulated in United Arab Emirates? What are the requirements for responding to data breaches?

This is not specified under any UAE law. The Penal Code does contain a provision that requires a report of a crime to be made to the police, although this is not always done in practice.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

There is, as noted, a general constitutional right to privacy.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

There are restrictions relating to "spam" that can be considered. Marketing communications are regulated by the Telecommunications Regulatory Authority under its Unsolicited Electronic Communications Policy dated December 30, 2009 ("Spam Policy") and the associated Mobile Spam Annex.

The Spam Policy requires consent from recipients in two specific scenarios:

(a) The first is where marketing communications are to be sent by the two locally licensed telecoms service providers.

(b) The second, under the Mobile Spam Annex, refers to marketing communications that are sent by bulk SMS service providers who have contracted with licensed telecoms service providers to send messages.

Outside of these two specific scenarios, other organizations that send marketing communications are not subject to any regulation requiring consent. The Spam Policy does require licensed telecoms service providers to take all practical measures to end the transmission of unsolicited marketing electronic communications (being defined as marketing electronic communications sent without the consent of the recipient).

Ultimately, obtaining the consent of the recipient would limit any risk in the UAE, albeit that the risk can be considered small. As noted above, the Spam Policy does not apply directly to senders who are not locally licensed telecoms service providers or bulk SMS service providers under contract with a locally licensed telco.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

This is not specifically addressed under any UAE law.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

This is not specifically addressed under any UAE law.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

This is not specifically addressed under any UAE law. The law would, as noted above, require a general consent.

8.5 Are there specific privacy rules governing data brokers?

This is not specifically addressed under any UAE law.

8.6 How is social media regulated from a privacy perspective?

This is not specifically addressed under any UAE law.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

This is not specifically addressed under any UAE law. In general, we find that many loyalty programs have accumulated large databases from various sources, and continue their use on the basis that the spam laws detailed above are not actively enforced.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

This is not specifically addressed under any UAE law. The terms of Article 380 (bis) of the Penal Code (see question 1.2(b)) do, however, imply that consent may be needed to "distribute or provide another person with … information or data or any other such things that he examines by virtue of his profession". This would, on an ordinary interpretation, potentially cover any transfer, whether within the UAE or outside of it.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

This is not specifically addressed under any UAE law.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

(a) These can be criminal in nature:

(i) Under the Penal Code Article 379: "Any individual who, by reason of his profession, craft, circumstance or art is entrusted with a secret and who discloses it in cases other than those permitted by the law, or who uses it for his own advantage or another person's advantage, shall be punishable by imprisonment for a minimum period of one year and/or by a fine of at least 20,000 Dirhams, unless the individual to whom the secret pertains has consented that it be disclosed or used. The punishment shall be imprisonment for a period not exceeding 5 years if the perpetrator is a public servant or an officer entrusted with a public service to whom the secret has been confided during, because of or by reason of performing his duties or services."

In addition, Article 380 (bis) adds: "Detention shall be inflicted upon whoever unrightfully copies, distributes or provides another person with the content of a phone call or message or information or data or any other such things that he examines by virtue of his profession".

(ii) Article 2 of the Cyber Crimes Law provides that gaining access to a website, an IT system or computer network without authorization (or in excess of authorization) is punishable by imprisonment and/or a fine of between AED 100,000 and AED 300,000.

If such access results in (amongst other things) disclosure of any data or information, then the punishment shall be imprisonment for a period of at least 6 months and/or a fine of between AED 150,000 and AED 750,000, or at least 1 year and/or a fine of between AED 250,000 and AED 1 million if the disclosed information is personal data.

(iii) Article 22 of the Cyber Crimes Law provides that unauthorized use of any IT system to disclose confidential information obtained during the course of employment shall be punished by imprisonment for a period of at least 6 months and/or a fine of between AED 500,000 and AED 1 million.

(b) There are also civil actions:

(i) The Civil Code allows for recovery of damage for any tortious act, and this would include the harm done because of misuse of a person's data. Article 282 is broadly phrased:

> "Any harm done to another shall render the actor, even though not a person of discretion, liable to make good the harm."

The data subject has three years to lodge a claim. It is important to note that the UAE courts require absolute proof of damage, and the damage must be attributable to the tortious act.

We note that the availability of criminal sanctions means that civil actions are not often sought — we see few such cases in action.

(ii) In addition, the Civil Code has provisions that apply to employees in particular. They are required, under Article 905 to "keep the industrial or trade secrets of the employer, including after the termination of the contract, as required by the agreement or by custom". In practice, we see most employers including a contractual term to augment this provision. The Article is limited in scope by the fact that the employer must prove the damage that arises, as is the case for all actions under the Civil Code.

(iii) Federal Law No 18 of 1993 on the Commercial Transaction Law also provides that traders may not seek to elicit secrets from their competitor's employees (under Article 64). Article 224 applies a similar obligation on an agent acting for a principal.

10.2 Do individuals have a private right of action? What are the potential remedies?

As individuals are able to report violations to the police, prosecutions would be undertaken by the police prosecution, rather than by an individual. With adequate proof of damage and the causal link between the damage and the act of disclosing the information in question, a civil action could be taken under UAE law.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of United Arab Emirates which affect privacy?

There are none.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

There is an expectation that a comprehensive data protection regime will be introduced in the UAE in the very near future. Sources have noted that the current draft will replicate the system implemented under the GDPR, following the lead of other countries in the region.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in United Arab Emirates?

At this stage, pending the new laws, there is nothing else to know.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

We have seen some interesting cases relating to privacy, in particular relating to the failure to obtain releases from people who are featured in audio-visual content. This issue reflects the importance placed on privacy by the government. However, the cases are generally related to the use of people's images without consent and do not reflect the data protection matters that are being seen in other countries at this time.

12.2 What do you envision the privacy landscape will look like in 5 years?

We expect that in 5 years' time there will most definitely be a federal law that addresses issues of data protection, and that it will reflect the general scope and operation of the GDPR provisions. This sort of legislation has already been introduced in neighboring countries such as Bahrain.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

We see the introduction of the anticipated new laws as being particularly problematic for entities that have been operating in the region for some years, as they are not yet accustomed to considering the importance of data protection. Businesses that are not already in the process of auditing and analyzing their data and their use of data may find themselves being unable to use or keep certain data that they have been using for some years. This is particularly challenging for the large number of small and medium sized companies ("SME"s) in the UAE. Our recommendation to all companies is to start this process as early as possible, and certainly before any laws come into force.

UNITED KINGDOM

1 PRIVACY LAW

1.1 How is privacy regulated in the United Kingdom?

The primary privacy legislation in the United Kingdom is the General Data Protection Regulation ("GDPR"). As an EU regulation, it currently has direct effect in the United Kingdom, and is also implemented in UK law through the UK Data Protection Act 2018 ("DPA 2018").

The UK government has issued the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 which amend the DPA 2018 so that it will work in a UK context after the United Kingdom leaves the European Union ("Brexit"). In practice there will therefore be little change to the core data protection principles, rights and obligations found in the GDPR immediately after Brexit.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") implements Directive 2002/58/EC (the "ePrivacy Directive") in UK law (see the European Union chapter). Currently, a draft of an ePrivacy Regulation ("ePR") is being considered as a replacement for the ePrivacy Directive. Once in force, it will be directly applicable in the Member States. However, if this is finalized after Brexit (and after any transition period) the ePR will not automatically form part of UK law (subject to any agreement between the European Union and the UK government). How the law in this area will evolve is therefore unclear at the time of writing.

Although this note focuses on the GDPR and PECR, 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.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The primary laws are those set out in the GDPR — please see the European Union chapter.

The GDPR regulates all aspects of the processing of personal data, from its collection, to its treatment, security and storage, through to 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.

The DPA 2018 has supplemented the GDPR in areas which provided for national derogations. For example, it:

(a) stipulates additional conditions and safeguards for processing special category and criminal offense data in a number of scenarios (see question 3.2); and

(b) adds exemptions to various parts of the GDPR, including in relation to data subjects' rights, and the transparency obligations in Articles 13 and 14 (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 GDPR and provide for specific rules that apply in relation to electronic communications. These rules apply irrespective of whether personal data is processed for the purposes of the electronic communication. For more information about the PECR, please see question 8.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The Information Commissioner's Office ("ICO") is the supervisory authority for the United Kingdom. It enforces breaches of privacy legislation through regulatory action, as well as issuing its own guidelines on how to comply with the GDPR in practice. The ICO has investigatory and corrective powers, including the power to impose a fine in respect of violations of the GDPR. At present, regulatory action (in particular fines) is the main concern for most businesses when thinking about GDPR compliance.

Nevertheless, it is also possible to bring claims for breach of the GDPR in the United Kingdom's civil courts — this is the mechanism by which individual data subjects are able to obtain financial redress. Whilst such claims have been relatively rare, the prospect of litigation by large groups of claimants following a recent decision of the Court of Appeal will likely make them a far bigger concern for data controllers going forward. These claims are of particular relevance for controllers processing the personal data of large numbers of data subjects.

2 SCOPE

2.1 Which companies are subject to privacy law in the United Kingdom?

See the European Union chapter for information on the material scope of the GDPR.

2.2 Does privacy law in the United Kingdom apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

See the European Union chapter for information on the territorial scope of the GDPR.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in the United Kingdom?

See the European Union chapter for the GDPR definition of "personal data", which is the applicable definition in the UK.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

See the European Union chapter for what data is considered "special" under the GDPR — this is applicable in the UK, albeit that the UK opted for a lower age for children to give their consent in relation to information society services: 13 years.

Please note that the DPA 2018 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).

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

See the European Union chapter.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

See the European Union chapter.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

See the European Union chapter.

In addition, the ICO has produced its own guidance on many of these topics (eg, on the transparency requirements under Articles 13 and 14; how to maintain an Article 30 record; when to conduct a data protection impact assessment ("DPIA"); how to deal with data breaches; and compliance in relation to direct marketing and the use of cookies). This guidance provides an additional insight into what controllers must do in practice to comply with the GDPR and PECR.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in the United Kingdom? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

See the European Union chapter.

6.2 How are data breaches regulated in the United Kingdom? What are the requirements for responding to data breaches?

See the European Union chapter.

The ICO has produced additional guidance on data breach requirements, including when a breach may be notifiable under Article 33, when individuals should be informed under Article 34 and what to do where the data controller has only partial information about the breach available.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

See the European Union chapter.

It is worth noting that requests under Article 15 (data subject access requests) are more common in the United Kingdom than many other jurisdictions and the right to obtain copies of the personal data is taken seriously by the ICO.

In the United Kingdom, Article 15 requests are commonly used to try to obtain documents as a precursor to litigation, 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.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

See the European Union chapter for privacy law obligations.

In addition, the PECR sit alongside those privacy law obligations and provide for specific rules that apply in relation to electronic communications. These rules apply, irrespective of whether personal data is processed for the purposes of the electronic communication.

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 be of a "GDPR standard") from the recipient; or

(b) is able to rely on what is known colloquially as the "soft opt-in" or "existing customer" exemption (which is outside the scope of this chapter).

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 recently 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 facsimile, although these forms of communications are outside the scope of this chapter.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

See the European Union chapter. By way of clarification, where cookies and similar technologies store information or access information stored on user devices, the PECR requires user consent to be obtained. This is a separate requirement to having an Article 6 lawful basis for any processing of personal data by such technologies.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

See the European Union chapter.

At the time of writing, targeted and behavioral advertising activities — which involve the widespread collection, use and sharing of personal data amongst many different "adtech" service providers that sit between advertisers and online publishers — are being scrutinized by the ICO. These activities have also been the subject of complaints to the ICO from various privacy activists, who regard them as constituting an industry-wide data breach which exposes data subjects to alleged mass profiling and the risk of manipulation and discrimination.

In June 2019, the ICO issued a progress report setting out its initial concerns about the use of personal data in the ad tech sector — which was described as "immature in its understanding of data protection requirements" — in particular when it comes to real time bidding ("RTB"). The ICO gave industry six months to improve its data protection practices. If you would like to read more about this report, please visit https://www.lewissilkin.com/en/news/ico-update-report-into-ad-tech-and-rtb.

In January 2020, the ICO announced that, while it has observed improvement from some industry actors, it "will continue to investigate RTB" and that "it may be necessary to take formal regulatory action". This announcement did not, however, satisfy the complainants referred to above, whose lawyer alleged that "the ICO has failed to take direct enforcement action needed to remedy these breaches" and called for "proper judicial oversight" of the ICO.

It remains to be seen what, if any, formal regulatory action will be taken by the ICO, but we expect this to continue to be an area of focus for the foreseeable future. At time of writing, the latest ICO blog suggests regulatory action is imminent.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

See the European Union chapter.

In addition, the ICO has recently issued a draft direct marketing code of practice, which states that consent is usually the most appropriate lawful basis for the use of "custom audience" advertising. The ICO has not ruled out reliance on legitimate interests for such activities but, in the ICO's view, these activities are not in the "reasonable expectations" of data subjects and, therefore, organizations may find it difficult properly to establish legitimate interests as a lawful basis for such processing.

8.5 Are there specific privacy rules governing data brokers?

See the European Union chapter.

In addition, the ICO's recently issued draft direct marketing code of practice cautions organizations to "be very careful about using" direct marketing lists offered for sale, rent or license by data brokers and other organizations. In particular, care is needed as regards ensuring 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 contained in the list.

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 in the context of data protection obligations owed more generally (under the GDPR and PECR).

8.6 How is social media regulated from a privacy perspective?

See the European Union chapter.

In addition, given the propensity for social media to be used to direct targeted or behavioral advertising to individuals, including by the use of social media operated tracking technologies (such as "plug-ins") see also the response to questions 8.2 and 8.3.

Moreover, the ICO's recent draft direct marketing code of practice identifies the use of social media for the purposes of direct marketing as being an area of focus in the context of data protection obligations owed more generally (under the GDPR and PECR). In particular, the ICO has indicated that consent will usually be required to undertake "custom audience" advertising, and that direct marketing sent to an individual's social media inbox constitutes marketing via "electronic mail" (see question 8.1).

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

See the European Union chapter.

Again, however, loyalty schemes feature a number of times in the ICO's recently issued draft direct marketing code of practice. The profiling of personal data collected via the use of loyalty schemes is regarded by the ICO as a processing activity that is "likely to result in a high risk" to data subjects, triggering the GDPR requirement to undertake a DPIA.

In addition, where such profiling is "privacy intrusive" or may result in "significant risks" to a data subject, which would include discriminating against the data subject by causing them to pay a higher price for a product or service, such processing will not be "in an individual's reasonable expectations" and, as such, cannot be undertaken on the basis of the organization's legitimate interests (consent will be required).

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

See the European Union chapter.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

See the European Union chapter.

In addition, as a result of its exit from the European Union, the United Kingdom will become a "third country" insofar as the European Union is concerned. Consequently, following the expiry of the "transition period" (currently set to take place on December 31, 2020), transfers of personal data from the European Economic Area ("EEA") to the United Kingdom will be treated the same as transfers of personal data from the European Union to other non-EU territories. Unless such transfers are exempt, they will only be lawful if the United Kingdom achieves an adequacy decision from the European Commission or (absent such a decision) appropriate safeguards (eg, standard contractual clauses) are in place in respect of the transfer.

There have been conflicting reports over the likelihood that the United Kingdom will be granted adequacy status. Ultimately, the decision is a political one, and will likely form part of the overall negotiation of the future relationship between the United Kingdom and the European Union. At present, there is little reason to assume that adequacy status will be denied. Organizations should, however, continue to monitor and be prepared to implement appropriate safeguards should the need arise.

Finally, transfers of personal data in the opposite direction — ie, from the United Kingdom to the EEA — are not expected to be affected in a similar way. The UK government has taken a pragmatic approach by indicating that it will not treat any such transfers as being restricted and that no additional safeguards will be necessary (though, again, this is a political matter and is subject to change). On a similar note, adequacy decisions and safeguards that can be relied on to transfer personal data outside the EEA (eg, standard contractual clauses and Privacy Shield certifications) are expected to be "adopted" by the United Kingdom, so that they can be relied on to transfer personal data from the United Kingdom to non-EEA territories.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

See the European Union chapter.

10.2 Do individuals have a private right of action? What are the potential remedies?

See the European Union chapter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of the United Kingdom which affect privacy?

None.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The ICO is currently investigating the adtech industry in respect of its compliance with the GDPR. Please see further question 8.

In addition, the draft ePR is also a hot topic. Please see the European Union chapter.

Finally, the United Kingdom's withdrawal from the European Union ("Brexit") has the potential to have a significant impact on data protection, in particular in respect of the transfers of personal data from the EEA to the United Kingdom (which may become "restricted transfers"). However, few far reaching consequences are expected during the implementation period (which will last until at least December 31, 2020). If you would like to read more about Brexit's impact on data protection, please visit https://www.lewissilkin.com/en/campaigns/brexit/data-privacy.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in United Kingdom?

None in particular.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

See the European Union chapter.

One trend that we have observed is a greater propensity for individuals to "weaponize" their privacy rights, and to bring civil claims in small claims courts for purported (and relatively minor) violations of data protection and ePrivacy law, in particular in respect of direct marketing activities.

12.2 What do you envision the privacy landscape will look like in 5 years?

See the European Union chapter.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

See the European Union chapter.

From a local perspective, although the GDPR purports to harmonize EU data protection laws, companies operating across borders will face uncertainties as national supervisory authorities and courts interpret the GDPR's requirements. Although the United Kingdom has committed to maintaining a parallel regime in the wake of Brexit, it remains to be seen whether this will hold true, especially as the United Kingdom is unlikely to recognize decisions of the Court of Justice of the European Union as being binding on it. In any event, it will take some years for these uncertainties to subside.

We also envisage that data transfer mechanisms — in particular Standard Contractual Clauses and Privacy Shield (both the EU-US and UK-US version) — will come under further attack from privacy activists.

UNITED STATES OF AMERICA

1 PRIVACY LAW

1.1 How is privacy regulated in the United States?

US privacy is regulated through a patchwork of federal, state and sector-specific privacy laws and self-regulation. There is no single comprehensive data privacy framework similar to Europe's General Data Protection Regulation ("GDPR"). California recently enacted the California Consumer Privacy Act of 2018 ("CCPA"), which is currently the most comprehensive privacy law in the US.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Below are some key privacy laws relevant to advertising practices:

(a) Federal Law

(i) Federal Trade Commission Act ("FTC Act"): The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC Act was not specifically designed to regulate privacy; however, the Federal Trade Commission ("FTC") has brought a wide range of privacy and data security related enforcement actions against companies based on alleged violations of the FTC Act.

(ii) Children's Online Privacy Protection Act ("COPPA"): COPPA regulates the online collection of information from children, and is perhaps the most important US privacy law for the advertising industry. The law prohibits companies from knowingly collecting personal information from children under 13 without verifiable parental consent unless an exception applies.

(iii) Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM"): CAN-SPAM regulates the use of commercial emails. The law requires companies to allow individuals to opt-out of receiving marketing emails, among other things.

(iv) Telephone Consumer Protection Act ("TCPA") and Telemarketing and Consumer Fraud and Abuse Prevention Act: These laws regulate telemarketing activities, such as telephone calls and text messages. Notably, TCPA prohibits companies from making calls or sending texts without prior express consent.

(v) Video Privacy Protection Act ("VPPA"): VPPA regulates information that identifies an individual as having requested or obtained specific video materials or services. The law prohibits companies from knowingly disclosing such information without prior consent, and is relevant to video streaming and online integrations.

(vi) Health Insurance Portability and Accountability Act ("HIPAA"): HIPAA regulates the use and disclosure of protected health information by health care providers, health plans, and health care clearinghouses, as well as companies that perform services on behalf of these entities, such as advertising agencies.

(vii) Fair Credit Reporting Act ("FCRA"): FCRA regulates companies that compile and sell reports regarding consumer eligibility for certain benefits and transactions, as well as companies that use those reports. Advertisers arguably could become subject to FCRA depending on their use of third-party data.

(viii) Gramm-Leach-Bliley Act ("GLBA"): GLBA regulates the use of nonpublic personal information collected by financial institutions in connection with providing financial products or services, as well as companies that receive such information, such as advertising agencies.

(ix) Family Educational Rights and Privacy Act ("FERPA"): FERPA regulates the processing of student information.

(b) State and Municipal Law

(i) California Law: California leads the US in setting data privacy and security standards, and has inspired similar or near identical legislation in other states.

(1) California Online Privacy Protection Act ("CalOPPA"): Considered the nation's first online privacy law, CalOPPA requires businesses that collect the personal information of California residents from websites, apps, or other online services to post and honor their privacy policies.

(2) California Consumer Privacy Act ("CCPA"): The CCPA is California's new comprehensive privacy law that imposes robust obligations on businesses that process the personal information of California residents, and provides California residents with the rights to know, delete, and opt-out of the sale of their personal information to third parties. The law also regulates service providers and other third parties that receive personal information from businesses.

(3) California "Shine the Light": This law requires businesses to disclose certain information regarding how they share personal information of California residents with third parties for those third parties' own direct marketing purposes.

(4) Privacy Rights for California Minors in the Digital World Act ("Eraser Law"): This law requires businesses to permit minors who have an online account with the business to remove from public view content posted by them through their account.

(5) Song Beverly Credit Card Act: This law regulates the collection of personal identification information in connection with credit card transactions.

(6) Student Online Personal Information Protection Act: This law prohibits the sharing of certain student information for targeted advertising purposes.

(ii) Nevada Sale Law: This law gives Nevada residents the right to opt-out of the sale of their covered information.

(iii) Data Broker Laws: Vermont and California have laws requiring data brokers to register with the state on an annual basis.

(iv) Biometric Privacy Laws: Several states and municipalities have biometric privacy laws, the most notable of which is the Illinois Biometric Privacy Act ("BIPA"). BIPA prohibits companies from collecting or using biometric information without prior consent.

(v) Consumer Protection Laws: All 50 states have laws analogous to the FTC Act that prohibit unfair or deceptive acts or practices.

(vi) Other Sectoral Laws: Many states and municipalities have laws governing specific types of information such as video, health, financial, and student information.

(vii) State Data Breach Laws: All 50 states and US territories have data breach notification laws.

(c) Self-Regulation

(i) Interest-Based Advertising: The FTC and advertising trade groups, including the Digital Advertising Alliance ("DAA") and Network Advertising Initiative ("NAI"), have developed self-regulatory principles regarding behavioral advertising.

(ii) Children: The Children's Advertising Review Unit ("CARU") has developed self-regulatory guidelines addressing children's advertising and the collection and use of information from children.

Please see subsequent responses for additional information on certain of these key laws.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

(a) Federal Regulators: The FTC is viewed as the chief federal agency on privacy. The FTC has brought a wide range of privacy and data security related enforcement actions against companies based on alleged violations of Section 5 of the FTC Act, including for failure to comply with posted privacy policies, give consumers adequate notice and choice over their information, and maintain reasonable security to protect information. The FTC does not have jurisdiction over certain commercial activities, including with respect to banks, common carriers (eg, telecommunications companies), and non-profits.

In addition, there are a number of sectoral-specific enforcement authorities. For example, the Department of Health and Human Services ("HHS") primarily enforces violations of HIPAA, the Consumer Financial Protection Bureau ("CFPB") primarily enforces violations of GLBA, and the Federal Communications Commission ("FCC") primarily enforces violations of the Communications Act.

(b) State Regulators: State Attorneys General are the primary enforcement authorities at the state level. State and municipal agencies may also enforce violations of law.

(c) Self-Regulatory Bodies: Self-regulation is not binding legal authority. However, violations of self-regulation may result in a revocation of membership or the applicable self-regulatory body referring the alleged violator to the FTC or applicable State Attorney General. The Better Business Bureau ("BBB") is particularly notable since it enforces violations of the DAA self-regulatory principles.

(d) Private Right of Action: Individuals may bring lawsuits against companies for alleged privacy violations. Many privacy laws include an express private right of action and allow for individuals to bring a class action on behalf of numerous affected individuals. Lawsuits are most successful where the law provides for statutory damages that do not require the individual to demonstrate actual harm. TCPA, VPPA, BIPA, and the data breach provisions of the CCPA all provide for statutory damages.

2 SCOPE

2.1 Which companies are subject to privacy law in the United States?

Nearly any company that collects information from or about US residents will be subject, in some capacity, to the patchwork of federal, state, and sector-specific privacy laws and self-regulation. Companies need to consider a multitude of factors to determine which privacy laws apply. These factors include, among other things, the sector in which a company operates (such as healthcare), the types of information collected by the company, the jurisdictions in which the company operates, the location or residence of the individuals from or about whom information is collected, and the manner in which information is used and shared by the company. Companies engaged in advertising and marketing practices should particularly evaluate COPPA, CAN-SPAM, TCPA, CCPA, data breach laws, and self-regulatory guidelines.

2.2 Does privacy law in the United States apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, a company not located in the US may be subject to US privacy law. Determining the extraterritorial jurisdiction of US privacy law is a fact-specific inquiry. For example, US privacy law may apply to a company that conducts business in the US, directs its products or services to the US, owns or licenses information of US residents, or otherwise has a nexus with the US, even if the company does not have physical operations in the US.

As a specific example, the CCPA regulates businesses. Under the CCPA, a "business" is defined as a for-profit entity that collects personal information from California residents, determines the purposes and means of processing, does business in the state of California, and meets one of the following thresholds:

(a) annual gross revenue that exceeds $25 million;

(b) annually buys, receives, shares, or sells the personal information of more than 50,000 California residents, households, or devices for commercial purposes; or

(c) derives 50% or more of annual revenues from selling California residents' personal information.

The phrase "does business in the state of California" is very broad, and arguably could subject companies based outside the US to the California law.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in the United States?

The US does not have a uniform definition of "personal information". Each federal and state privacy law has its own definition, and the data elements captured by the definition vary greatly depending on the law. However, US privacy law is quickly moving toward broad GDPR-like definitions. Under the CCPA, "personal information" is defined as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This means that information that historically has been treated as personally identifiable (such as names, email addresses, and phone numbers) as well as information that historically has not been treated as personally identifiable (such as IP addresses, Ad Ids, and geolocation data) all may fall within the definition of personal information, and be subject to privacy obligations.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

The US does not have a uniform definition of "sensitive information". However, the FTC and other regulators have defined "sensitive information" to include children's information, video viewing information, health information, financial information, social security numbers, biometric information, and precise location data (eg, lat/long). These categories of sensitive information generally align with sector-specific privacy laws, including COPPA, VPPA, HIPAA, GLBA, and BIPA, as well as the self-regulatory guidelines from the DAA and NAI. As a general rule, the collection of sensitive information requires opt-in consent.

As an important note, COPPA's definition of "personal information" is very broad, and includes persistent identifiers (such as IP addresses and Ad Ids). Companies that deal with children's personal information (including where collected through online tracking technologies) should carefully evaluate COPPA's restrictions and obligations.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The FTC has identified five fair information practice principles:

(a) Notice and Awareness: consumers should be given notice of a company's information practices before information is collected from them;

(b) Choice and Consent: consumers should be given control over how their information is used. Under US law, most choice is opt-out;

(c) Access and Participation: consumers should have the ability to access their information and have the information corrected;

(d) Integrity and Security: information collected should be accurate and secure.; and

(e) Enforcement and Redress: consumers should be able to enforce noncompliance.

These core principles are a baseline, and subsequent federal and state laws, and self-regulatory guidelines have greatly expanded upon the principles. As an unofficial privacy principle, companies should also evaluate whether their practices pass the reasonable expectation test. In other words, would a reasonable individual expect the company to use their information in the way contemplated by the company? If the answer is "no" or the practice could be viewed as "creepy," then the company should re-evaluate the practice, as the practice could be deemed unfair or deceptive.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The US does not have a uniform means of assigning roles to companies based on how they process information. However, for many privacy laws, the company that controls the decision-making concerning the information, or is regulated by the applicable law, is responsible for ensuring both it and any recipients of the information comply with the law. Below are two examples of roles assigned by specific privacy laws:

(a) Under the CCPA, a company may take on one or more of three roles: a company is a:

(i) "business" if it meets the definition set out in question 2.2 above;

(ii) "service provider" if it processes California resident personal information on behalf of the business pursuant to a restrictive written contract and only for a "business purpose"; or

(iii) "third party" if it is neither the business nor a service provider.

The majority of the obligations under the CCPA apply to businesses. However, service providers share certain obligations, such as helping businesses effectuate the rights of California residents. The contract and relationship between a business and service provider is particularly important because if the contract or relationship does not align with the requirements of the CCPA, the service provider could be deemed a third party. Where a business sells personal information to another business or a third party, California residents have the right to opt-out of the sale of their personal information. While many businesses may not sell information in the traditional sense, the term "sale" is broadly defined under the CCPA, and this opt-out right arguably extends to disclosures of information in connection with targeted or behavioral advertising. Please see question 8.3 for more information.

(b) Under HIPAA, the regulated company is called a "covered entity." Covered entities are limited in scope, and only include health care providers, health plans, and health care clearinghouses. However, where the covered entity discloses protected health information to a company that performs services on its behalf, which is called a "business associate," the parties must enter into a business associate agreement designed to protect the information. Even without a contract, the business associate is subject to HIPAA obligations. Certain types of advertising and marketing may be restricted or entirely prohibited by HIPAA.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

Below are some key obligations required by privacy laws relevant to advertising practices:

(a) Privacy Policy: Companies must post and make readily available a privacy policy that clearly discloses their actual privacy practices, including the types of information collected, the purposes and manner in which such information is used and disclosed, the types of third parties to whom such information is disclosed, and their contact information. If a company makes material changes to its privacy policy, the company must provide additional notice. CalOPPA, CCPA, and other privacy laws set out specific disclosure obligations.

(b) Contracts: For certain types of information, companies must enter into contracts with their clients and/or service providers governing processing of the information.

(c) Choice: Companies must give individuals choice with respect to their data practices, especially in connection with secondary use purposes such as advertising and marketing.

(d) Rights: In some jurisdictions, such as California, or with respect to certain types of information, companies must give individuals certain rights over processing of the information.

(e) Security: Companies must implement and maintain reasonable measures to secure information. In the event of a data breach, companies may be required to notify applicable regulators and individuals, and provide credit or identity reporting services.

(f) Training: In some jurisdictions, such as California, or with respect to certain types of information, companies must train employees regarding processing of information.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in the United States? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

(a) Federal Law: The FTC has brought data security related enforcement actions against companies based on alleged violations of the FTC Act. While the FTC has not issued formal data security regulations related to its Section 5 authority, companies should look to cease-and-desist orders, decisions, and reports issued by the FTC for guidance on what security-related business practices may subject companies to FTC enforcement.

In addition, requirements for data security vary by sector. Under the HIPAA Security Rule, the health care sector is required to implement appropriate administrative, physical, and technical safeguards to ensure the security of electronic protected health information. Under the GLBA Safeguards Rule, the financial sector is required to protect the security of nonpublic personal information with administrative, technical, and physical safeguards. Under FERPA, schools that receive federal funds are required to use reasonable methods to ensure appropriate access to educational records.

(b) State and Municipal Law: A handful of states have statutes that impose specific requirements related to data security. For example, Massachusetts and New York require companies that hold information about state residents to have a comprehensive data security program. Many other states, such as California, have statutes that generally require companies to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. "Reasonable security" is not a legally defined term, and companies should look to FTC, State Attorney General, and industry definitions of the term in orders, guidance, and reports to help address compliance.

(c) Self-Regulation: Data security is self-regulated in certain industries. Some industry policies are mandatory, while others are voluntary. Notably, the Payment Card Industry Data Security Standard ("PCI-DSS") is an industry-set standard that establishes mandatory security requirements for organizations accepting or processing payment transactions. PCI-DSS obligations are also codified by Nevada law.

6.2 How are data breaches regulated in the United States? What are the requirements for responding to data breaches?

(a) Federal Law: The US does not have a single comprehensive data breach law. Breach notification requirements are imposed primarily at the state level, as discussed below.

Certain sectors have their own data breach requirements. Under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which is part of HIPAA, covered entities must notify affected individuals, the HHS, and potentially media outlets following a breach. Under GLBA, a financial institution must notify affected customers as soon as possible after determining nonpublic personal information has been, or will be, misused. Under the Customer Proprietary Network Information ("CPNI") rule, telecommunications carriers must notify law enforcement and consumers following a security breach.

(b) State and Municipal Law: 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 that would permit access to the account. Many states have expanded the definition to include elements such 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.

(c) Self-Regulation: Some industry standards, such as PCI-DSS, include data breach notification obligations.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The US does not have a single comprehensive privacy law that provides individuals with rights over their information. Instead, individuals' rights depend on their status under certain federal and state laws. For example, under COPPA, parents have the right to review and delete their children's information. Under CAN-SPAM and TCPA, individuals have the right to exercise choice over their receipt of certain types of communications. Other applicable federal and state laws may provide individuals with additional rights.

California is the first state to provide individuals with GDPR-like rights over their personal information. Under the CCPA, California residents have the rights to know, delete, and opt-out of the sale of their personal information. In addition, California residents have the right not to receive discriminatory treatment for exercising any of their rights, and may designate an authorized agent to submit requests on their behalf. Other states are considering similar laws designed to give state residents rights over their information.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Marketing communications are primarily regulated as follows, although additional laws and industry standards may apply:

(a) Emails: CAN-SPAM regulates the sending of commercial emails, and gives individuals the right to opt-out of receiving marketing emails, among other things. CAN-SPAM does not include an express private right of action.

(b) Texts: TCPA regulates the making of calls or sending of texts. Unlike CAN-SPAM, TCPA gives individuals the right to opt-in to receiving calls or texts, and provides significant penalties for violations. An individual may sue on behalf of many individuals for statutory damages of up to $500 for each violation (or up to $1,500 for each wilful violation) of TCPA. As an example, if a company sends 10,000 texts without prior express consent, the company could be sued for $15 million. Companies should exercise caution when engaging in phone or text campaigns.

(c) Push Notifications: Push notifications are not regulated by either CAN-SPAM or TCPA.

It is important to note that marketing communications often involve the use of tracking technologies. For example, pixels may be embedded in a marketing email. Please see question 8.2 for more information on tracking technologies.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Tracking technologies are primarily regulated as follows:

(a) FTC and Consumer Protection Laws: There is no federal law that specifically regulates tracking technologies. However, the FTC has brought privacy and data security related enforcement actions against companies based on unfair or deceptive acts or practices with respect to the use of tracking technologies. The FTC has taken the position that a company's use of tracking technologies requires notice to individuals of the tracking technologies, choice to control such tracking, and maintenance of reasonable security to avoid unexpected and unauthorized use of information collected through the tracking technologies.

The FTC generally has indicated that choice means opportunity to opt-out. For the collection of more sensitive categories of information, such as video viewing information and precise location data, the FTC has indicated that choice requires opt-in consent. In addition, the use of tracking technologies for targeted advertising is held to a higher standard than the use of such technologies for other purposes, such as analytics. A company's use of tracking technologies in a way that an individual would not reasonably expect, such as using tracking technologies to collect precise location data in a flashlight app, could constitute an unfair or deceptive act or practice.

Similar to the FTC, State Attorneys General and other state regulators have brought actions based on unfair or deceptive acts or practices with respect to the use of tracking technologies, and have issued guidance on the topic.

(b) California: California specifically regulates tracking technologies. Under CalOPPA, a business must disclose any third-party tracking on its website and, if the business tracks across sites and over time, how the business responds to Do Not Track signals. CalOPPA does not specifically require a business to respond to Do Not Track signals; however, the CCPA includes provisions that arguably now require a business to respond to such signals.

(c) Sector-Specific Laws: Certain sector-specific laws fundamentally impact the use of tracking technologies. For example, COPPA's prohibition on the collection of personal information (which is defined to include persistent identifiers as well as a child's voice) from children under 13 may completely restrict the use of certain tracking technologies on websites, apps, voice platforms, and other online services directed toward children. Similarly, using tracking technologies to collect protected health information could be entirely prohibited by HIPAA.

(d) Self-Regulation: The DAA and NAI have established self-regulatory principles regarding behavioral advertising. The principles require that any company that engages in behavioral advertising (including through tracking technologies) provide:

(i) notice of its practices:

(ii) enhanced notice at or prior to the time of collection;

(iii) choice to opt-out of (or for certain types of data opt-in to) behavioral advertising; and

(iv) reasonable security to protect the information.

To help industry comply, the DAA and NAI have created mechanisms that allow individuals to opt-out of receiving targeted ads from their participants. The BBB enforces violations of the DAA self-regulatory principles.

The Interactive Advertising Bureau ("IAB") recently developed a framework and technical specifications designed to help businesses address their Do Not Sell obligations under the CCPA. This framework differs from the DAA and NAI opt-outs because it aims to restrict the use of information passed through tracking technologies, not just the display of targeted advertising.

Many opt-outs for tracking technologies rely on cookies, and companies should understand (and disclose to individuals) that opt-outs are limited based on the underlying technology. For example, a cookie-based opt-out only limits information related to a specific browser or device, and not across many devices. Additionally, companies should understand that these self-regulatory frameworks are not safe harbors and do not ensure compliance with the law.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Similar to tracking technologies, targeted and behavioral advertising are regulated through a combination of consumer protection laws, California law, sector-specific laws, and self-regulation. Please see question 8.2 for more information.

The CCPA will have a fundamental impact on targeted and behavioral advertising. Under the CCPA, California residents have the right to opt-out of (or, in limited circumstances, opt-in to) the sale of their personal information to third parties. When a California resident opts out, the business must stop selling the personal information, and notify all third parties to whom it sold the information after it received the request. The business must wait at least 12 months before requesting the California resident to opt back in.

Businesses should pay attention to the term "sale", as that term is not defined in the traditional sense. Under the CCPA, a "sale" means the renting, releasing, disclosing, making available, or transferring of personal information by a business to another business or third party for monetary or valuable consideration. The California Attorney General's Office has indicated that targeted and behavioral advertising are sales. Assuming the Attorney General's interpretation holds, businesses may be required to stop sharing, for targeted or behavioral advertising purposes, the personal information of any California resident who has opted out of the sale of their personal information. Because targeted advertising and behavioral advertising depend on the sharing of device identifiers and similar information throughout the ecosystem, the Attorney General's interpretation threatens advertising revenue models that rely on real time bidding and related technologies. This interpretation also creates complexity for advertiser-agency relationships where an agency is prohibited from selling personal information but also instructed to engage in media buys that involve targeted and behavioral advertising. The advertising industry is working on potential technological and contractual solutions to address these issues, although there is no consensus at this time.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Similar to tracking technologies, customer matching is regulated through a combination of consumer protection laws, California law, sector-specific laws, and self-regulation. Advertisers should provide notice in their privacy policies of their use of customer matching, and ways for individuals to exercise choice. Please see question 8.2 for more information.

In addition, there are several important considerations for customer matching:

(a) Anonymous Data: Advertisers often claim the information they provide for matching purposes is not personal information because it is anonymous or hashed. Be careful, because US privacy law broadly defines "personal information" to include information that advertisers historically have considered to be anonymous or deidentified. For example, hashed identifiers uploaded to Facebook or collected through pixels on a website or ad, or matched IDs received from LiveRamp, arguably are personal information under the CCPA.

(b) Source of the Data: Advertisers should consider how they obtained the information they provide for matching purposes. First-party data (such as data received directly by an advertiser through its website) and third-party data (such as data purchased from a data broker) carry different obligations. If the information is third-party data, the advertiser arguably could be deemed a data broker (see question 8.5 below). Further, an advertiser's customer-relationship management ("CRM") data is not necessarily all first-party data subject to the same law, as the advertiser may combine information from various sources in its database. For example, if an advertiser is a financial institution, the information it collects in the context of a loan application could be subject to GLBA, while the information it collects through its website could be subject to the CCPA. Sharing of certain types of information in connection with customer matching may require opt-in consent, or be restricted, or entirely prohibited by law.

(c) Receipt of the Data: Advertisers should consider whether they will receive any personal information back in connection with the customer matching, and what legal and contractual restrictions will be placed around the information.

8.5 Are there specific privacy rules governing data brokers?

There is no federal privacy law specifically regulating data brokers, although the FTC has repeatedly voiced concern about data brokers, and certain laws (such as FCRA) may impact data brokers.

Vermont and California each have laws that require data brokers to register with the state on an annual basis, and that impose additional obligations on such companies. "Data brokers" are generally defined as companies that obtain information about an individual from a source other than the individual and sell or license that information to third parties. Data brokers that fail to register or comply with the law face penalties. Advertisers that do not traditionally act as data brokers should evaluate the applicability of the data broker requirements; the receipt and transmission of third-party data could arguably make the advertiser a data broker.

8.6 How is social media regulated from a privacy perspective?

Social media is regulated through a combination of the privacy laws set out in question 1.2. Where a company collects personal information through a social media platform (including on the company's brand page, through a chatbot, or publicly available on the platform), such collection is governed by

the company's privacy policy, as well as the terms and policies of the relevant social media platform. It is important to note that information collected through a social media platform is generally not considered publicly-available information. Companies should carefully review social media platform terms before collecting any information from the platform.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs and promotions are regulated through a combination of the privacy laws set out in question 1.2. Participants should be provided with notice of how their information is processed in connection with the loyalty program or promotion (such as through a link to the company's privacy policy when the participant first enters the program or promotion), and should be required to affirmatively opt-in to the program or promotion.

The CCPA includes specific provisions regarding financial incentives that may impact loyalty programs and promotions. Among the various obligations, a business must provide specific notice of any financial incentives it offers in exchange for personal information, and obtain opt-in consent to the financial incentive.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

US privacy laws do not specifically restrict the transfer of personal information outside the country. However, transfers may be restricted based on statements in an applicable privacy policy or by contract. Further, companies receiving personal data from the European Economic Area, Switzerland, or the United Kingdom may register with the Department of Commerce to receive the personal data pursuant to Privacy Shield. Please see the European Union chapter for more information.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

Companies should consider whether there are any contractual restrictions around the data transfer, and ensure the recipient company maintains reasonable security measures to protect the information. A data breach by the recipient company could result in significant liability.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

There are two categories of penalties for violations of privacy or data security laws in the US: penalties sought by regulators and penalties sought by individuals through private rights of action. Please see question 10.2 for information on penalties sought by individuals. As for penalties sought by regulators:

(a) Federal: The FTC may bring an action against a company for violations of the FTC Act. The FTC may seek remedies including cease-and-desist orders, disgorgement, restitution, and civil penalties. However, the FTC typically cannot seek civil penalties for first-time privacy or security offenses. The FTC generally can seek civil penalties only when there is a violation of a separate statute that establishes civil penalties, such as COPPA or FCRA. When a company is already subject to an FTC cease-and-desist order, violations of the order may result in significant civil penalties.

In contrast, sectoral law typically allows for monetary penalties for first-time offenses. CFPB, HHS, and FCC have all imposed penalties for privacy and data security violations on companies subject to their jurisdictions.

(b) State: In most states, the State Attorney General has broad authority over consumer protection and may seek both civil penalties and injunctive relief for privacy and data security violations under consumer protection statutes and data breach laws. While non-profits are not within the FTC's jurisdiction, penalties for non-profits are often applicable at the state level.

(c) Self-Regulatory: Violations of self-regulation may result in a revocation of membership or the applicable self-regulatory body referring the alleged violator to the FTC or applicable State Attorney General.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes, individuals in all states have private rights of action based on tort law. Most states allow individuals to sue under four primary tort theories:

(a) intrusion upon seclusion/solitude;

(b) public disclosure of private facts;

(c) appropriation; and

(d) false light.

The most common remedies in privacy tort cases are monetary damages and injunctive relief. Individuals may also sue based on theories of breach of contract or negligence. Some individuals have brought actions for violation of consumer protection laws based on violations of COPPA and other laws that do not provide an express private right of action.

Many state privacy and data security laws include an express private right of action. Although individuals may sue under such a private right of action, they often have difficultly establishing actual damages. For example, where an individual is involved in a data breach, that individual may not be able to demonstrate that the specific data breach directly damaged the individual's credit. Therefore, certain privacy and data security laws include statutory damages, meaning that individuals do not need to establish actual damages, but rather that the activity took place. TCPA, VPPA, BIPA, and the data breach provisions of the CCPA all provide for statutory damages. Companies involved in call or text message campaigns, the processing of video viewing information or biometric information, or the collection of information from California residents should be extra diligent in evaluating the risks.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of United States which affect privacy?

The First Amendment to the US Constitution reflects the importance that US citizens place on information dissemination, which can create tensions with privacy. In the US, First Amendment protections extend to both individuals and companies, all of whom are granted the right to freedom of speech. In contrast, the US Constitution does not include an explicit right to privacy, although the Fourth Amendment and case law have alluded to such a right. Also, a number of states have codified a right to privacy. This tension between the right to freedom of speech and privacy has resulted in numerous cases where a plaintiff asserts a right to privacy while the defendant relies on the First Amendment. While the First Amendment is not a complete defense, unlike other jurisdictions, the right to freedom of speech is generally considered more important than the right to privacy.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The CCPA is the first GDPR-like privacy law in the US, and other states are expected to follow with their own comprehensive privacy laws. Absent a change in the federal legislative landscape, privacy law in the US may become similar to data breach law, with companies needing to comply with over 50 different privacy laws. In addition, the proponents of the CCPA have put forth a new initiative called the California Privacy Rights Act ("CPRA"), which would add new obligations for companies that process personal information of California residents. The CPRA is set to be on the November 2020 election ballot for California.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in the United States?

The US may be viewed as more litigious than other jurisdictions, in part due to the existence of class actions. A class action is a lawsuit filed against a defendant by a group of individuals. In areas of privacy law where private rights of action provide for statutory damages, attorneys actively pursue class actions.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Privacy awareness and concern in the US has significantly increased over the past few years, which has led to changes in behavior and increased regulation. This can be attributed to several significant events:

(a) First, in September 2017, Equifax experienced a data breach that affected over 147 million people.

(b) Second, in March 2018, US citizens became aware that a political data analysis firm called Cambridge Analytica improperly obtained the information of over 87 million people from Facebook's platform for purposes of influencing voter behavior and elections.

(c) Third, in May 2018, the GDPR took effect, which provided rights to individuals located thousands of miles away but not to those in the backyard of Silicon-Valley based technology companies.

Through a combination of these events, US citizens realized the dangers associated with "Big Data" and the lack of transparency and choice over the use of their information. As a result, a number of states, including California, have since enacted or considered laws intended to provide individuals with greater transparency and choice over the use of their information.

12.2 What do you envision the privacy landscape will look like in 5 years?

Most individuals in the US will have privacy rights within 5 years. Based on the current legislative landscape, privacy law will be governed at the state level, and each state will have its own comprehensive privacy law. There is a possibility that the US will pass a comprehensive federal privacy law, but, as at the time of writing, it is unlikely that the law will preempt or be more stringent than state law.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

The current patchwork of privacy law requires companies to comply with numerous laws, many of which conflict or are ambiguous. Further, the ad tech industry is rapidly changing due to the restrictions imposed on the processing of personal information. Google and other web browser providers are severely limiting tracking technologies that allow for the collection and sharing of third-party data, and companies will need to rely more on first-party data for their advertising initiatives. Limiting access to third-party data may strengthen large publishers while weakening small players and companies that have few touch points with individuals.

URUGUAY

1 PRIVACY LAW

1.1 How is privacy 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, UDPR, are also applicable, such as the guidelines for the use of video surveillance, drones or cookies, or the guidelines for data dissociation.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The key regulations on personal data protection in Uruguay are the following:

(a) Law No 18, 331 on the Protection of Personal Data and Habeas Data Action (the "Law") and its Regulatory Decree No 414/009;

(b) Law No 19,670 on Rendering of Accounts and Balancing of Budget Execution of the Exercise 2017 and its Regulatory Decree No 64/020;

(c) Regulatory Decree No 396/003 regarding electronic medical record; and

(d) Regulatory Decree No 664/008, which creates the registry of databases.

There are no special regulations on data protection aspects for advertising activities.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Uruguay's data protection regulator is the Regulatory and Personal Data Control Unit (*Unidad Reguladora y de Control de Datos Personales*, "UDPR"). UDPR is an autonomous entity of the Agency for the Development of Electronic Government and the Information-Based Society (*Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento*, "AGESIC").

There are currently no self-regulatory bodies on the matter.

2 SCOPE

2.1 Which companies are subject to privacy law in Uruguay?

All companies that meet the requirements for the application of the Law 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 Law, where appropriate.

2.2 Does privacy law in Uruguay apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

The Law 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 Law 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 Law particular to companies outside Uruguay.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined 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 a piece of information not to be considered personal data, UDPR considers that it must be irreversibly dissociated.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"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 Law 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, among other hypotheses, processing sensitive data as its main business is one of the cases under which a company must appoint a data protection officer before UDPR. 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 of carrying out a privacy impact assessment.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

According to the Law, data controllers, and all those processing personal data of third parties, must comply with the following principles:

(a) Legality: Data controllers have the obligation to register a database before UDPR 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 or in a manner contrary to the provisions of UDPR.

(c) Purpose Limitation: Personal data must not be used for purposes that are different 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.

The UDPR allows certain exceptions to the limitation on retention, such as when the data has value for historical, statistical, or scientific reasons.

(d) Prior Consent: As a general rule, the processing of personal data is permitted only if the data subject has given his/her free, prior, explicit and informed consent, which must be documented. There are certain exceptions to the principle, such as:

(i) when the data comes from public sources of information, such as registries or publications in mass media;

(ii) when the data is collected for the performance of functions of the government or under a legal obligation;

(iii) for listings of natural persons, those that are limited to names, identity document, nationality, address, and date of birth regarding natural persons, or, in the case of legal entities, limited to corporate name, brand name, tax identification number, address, phone number, and identity of the people in charge;

(iv) when the data derives from a contractual, scientific or professional relationship of the data subject, and is necessary for its development or execution; or

(v) when the treatment is carried out by a natural person for his/her own personal and domestic use.

(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.

(g) Responsibility: The data controller and the data processor are responsible for the violation of any provision of the Law. 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 Law also states that both data controllers and data processors must take all the appropriate technical and organizational measures (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.

In addition, although there are no specific provisions to that effect in the Law, when carrying out data processing activities, note that 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 this documentation of the measures must also be met.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

The Law 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 UDPR in compliance with the principle of legality, not the processor. However, in general terms, the obligations provided in the Law extend to both data controllers and processors.

Regarding contractual requirements, note that, although the use of data processing agreements is highly recommended in order to formalize the obligations and responsibilities of each party (especially in order to comply with the principle of proactive responsibility), in Uruguay there is no specific obligation to do so. Thus, there are no particular contractual requirements to be included by a data processor or a data controller.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

The key obligations under the Law are the following:

(a) registering the databases before UDPR;

(b) complying with the principles stated in the Law (see question 3.3);

(c) responding as required to data subjects when they exercise any of their rights under the Law (see question 7.1);

(d) 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 his/her consent;

(e) informing data subjects about their right to request the block or removal of their personal information from marketing and advertising listings;

(f) appointing a data protection officer before UDPR, 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). The main functions of a data protection officer are:

(i) to advise on the design and appliance of privacy policies,

(ii) to oversee the fulfilment of the data protection framework,

(iii) to recommend any measurements to comply with the international framework and standards regarding privacy, and

(iv) to act as a point of contact between its entity and UDPR;

(g) carrying out privacy impact assessments in those cases required by the Law or when UDPR deems it convenient;

(h) implementing privacy by design and by default measures;

(i) when processing personal data through a website, making the privacy policy about the data processing available;

(j) when a data breach occurs, initiating the necessary procedures to minimize the impact of said incidents within the first 24 hours of verification; and

(k) notifying data securities breaches to UDPR within 72 hours and also to the data subjects.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Uruguay? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Under the principle of data security (see question 3.3), 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 required. However, AGESIC recommends the implementation of the ISO/IEC standards regarding information security. To that end, a set of guidelines for the enforcement of the Law according to the ISO/IEC standards has been developed for organizations to use as recommendations to comply with the Law. In addition, Decree No 64/020 states that the implementation of national and international standards on data security will be well be appreciated, such as the Framework for Cybersecurity prepared by the Agency for the Development of Electronic Government and the Information-Based Society ("AGESIC") (of which UDPR is a decentralized body).

The adopted measures must be documented and periodically reviewed, and their effectiveness must be analyzed. The documentation must comply with certain requisites, such as include the means and purpose of the data processing, among others. The documents should be available on request of UDPR.

6.2 How are data breaches regulated in Uruguay? What are the requirements for responding to data breaches?

According to the Law, a data security breach must be reported immediately, in detail, by both data controllers and data processors, as soon as they become aware of the breach.

The Law states that the concept of "security breach" includes, among others, breaches that cause the disclosure, destruction, loss or accidental or unlawful alteration of personal data, or unauthorized communication or access to such data.In case 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 UDPR within 72 hours and to all affected data subjects, and must include details about the breach and the measures taken. The Law provides that UDPR will coordinate the course of action to be taken with the National Centre for Response to Computer Security Incidents of Uruguay ("CERTUy").

In case a data processor becomes aware of a data breach, he/she must immediately inform the data controller of the situation. The controller will then notify those data subjects whose rights have been significantly affected.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Data subjects have the following rights regarding their personal data, though subject to certain conditions:

(a) the right to access;

(b) the right to suppress (delete);

(c) the right to update;

(d) the right to rectify;

(e) the right to include; and

(f) the right to information.

Among other aspects, please note that the data controller must respond to the request of a data subject within five business days. Otherwise, the data subject may start an action in *habeas data*.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The Law states that, in the collection of addresses, the distribution of documents, advertising, commercial prospecting, sale 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 provided that the personal information appears on publicly accessible documents or is provided by the data subjects themselves or obtained with their consent.

The Law 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 his/her data from the databases.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The Law does not specifically refer to tracking technologies.

However, on the one hand, as long as the technologies process personal information, the Law and its provisions will apply.

On the other hand, in October 2018, UDPR 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 Law apply when implementing cookies, as does the data subjects' 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 guarantee 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 different or incompatible purposes to those for which it was collected.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Please see question 8.1.

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, among others.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The Law states that the communication of personal data to a third party can only be done for purposes directly related to the legitimate interest of the sender and recipient, and only with the prior consent of the data subject.

Regarding consent, the Law provides that the data subject must 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. It also states that consent is revocable.

By way of reference, note that when referring to consent for data processing, Decree No 414/009 states that the data subject must be provided with a simple, clear and free of charge way to give or refuse their consent. In that regard, it is understood that the obligation of obtaining the consent is fulfilled when the data subject is given the possibility to choose between two clearly identified options, which cannot be pre marked, whether in favor or against.

Finally, note that prior consent for communicating personal data is not necessary in the following cases:

(a) when provided by a law of general interest;

(b) when consent is not required for data processing;

(c) regarding health data, when the communication is necessary for health or emergency reasons, or for carrying out epidemiological studies, as long as the data subjects' identity is preserved by using adequate dissociation mechanisms when applicable; or

(d) when the personal data is dissociated, so the data subjects are not identifiable.

8.5 Are there specific privacy rules governing data brokers?

In Uruguay there are no particular privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

In Uruguay there are no particular data privacy rules governing social media.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There are no particular data protection provisions regulating loyalty programs and promotions. However, the Law will apply in cases where personal data is processed in such programs or promotions.

Also note that, by Resolution No 64/2013 of UDPR, every website that carries out data processing in Uruguay (such as when the enrolment to a loyalty program or promotion is done through a website) must publish the conditions related to such processing, in accordance with the Law.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The Law states that cross border personal data transfers to countries or international organizations that do not provide adequate levels of protection, according to the standards of international or regional law, are prohibited.

By Resolution No 4/2019 of UDPR, the countries that do provide adequate levels are 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. (Please note that, in 2012, Uruguay was granted the adequacy note for international transfer purposes by the European Commission, as local regulation has been deemed aligned with European regulatory standards.)

In addition, by Resolution No 4/2019, UDPR also considers data transfers to companies located in the United States that have adhered to the Privacy Shield Agreement to be lawful.

Finally, cross border data transfers carried out within a multinational company, between affiliates, between subsidiaries, and between them all and their parent company, are considered lawful as long as a code of conduct of professional practice on the matter is previously registered before UDPR.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

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 Uruguayan Central Bank ("UCB") may require the prior authorization of UCB. Among other aspects to be considered in such cases is whether the data processing abroad is considered substantial or not.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

UDPR 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 previous record of other infringements, or whenever the infringement is severe or very severe);

(d) suspension of the database concerned (when the infringement is very severe); and

(e) closing of the database concerned (when the infringement is very severe).

The sanctions of suspension and closing of databases are applied when a fine is not adequate to address very severe violations of the Law.

In general, though, UDPR does not, in practice, have a policy of active control; it acts upon claims submitted by data subjects.

10.2 Do individuals have a private right of action? What are the potential remedies?

The Law 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 Law, or

(b) when, a data subject having requested that their information be corrected, updated, removed, or deleted, such request was not complied with within the timeframe established by the Law.

The action of *habeas data* may be exercised by the data subjects concerned or 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 Law, data subjects can also submit civil actions regarding data privacy.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Uruguay which affect privacy?

No, we do not visualize particular rules that affect privacy which are particular to local culture.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The bill of a law of urgent consideration that includes changes in different areas will be discussed in Congress in the near future. Among other modifications, the bill includes a regulation on the right to be forgotten.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Uruguay?

The Law 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 him/her. A data subject may challenge administrative acts or decisions involving a personal evaluation of his/her behavior, the sole rationale of which is the processing of personal data that provides a definition of his/her characteristics or personality.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Local 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, which in Uruguay has been in force since 2009).

We also note that data subjects have become more aware of their rights under the Law, as well as the obligations of the data controllers/processors.

Finally, we have noticed that data subjects sometime use the Law for purposes other than those for which the Law 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 do you envision the privacy landscape will look like in 5 years?

We foresee that in the next 5 years compliance with local regulation will continue to increase, as will data subjects' claims before UDPR. We also expect that UDPR will initiate more ex officio investigations.

12.3 What are some of the 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 make privacy impact assessments, anticipating the risks of the data processing, and implementing security measures and mechanisms to show compliance to UDPR.

VENEZUELA

1 PRIVACY LAW

1.1 How is privacy 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 key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

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; and

(e) Special Law of Cybercrimes.

However, the solid principles established in the Constitution have not been developed in subsequent and specific laws.

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 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."

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

There is no specific administrative entity in charge of privacy matters.

Most privacy cases are decided in court and the courts will determine any applicable precautionary measures, depending on the specific case.

Another agency with possible jurisdiction in the administrative field is SUNDDE (this agency mostly deals with fair price issues, but also with a few consumer protection matters).

2 SCOPE

2.1 Which companies are subject to privacy law in Venezuela?

All entities conducting activities in Venezuela are subject to the constitutional principles.

2.2 Does privacy law in Venezuela apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, based on the constitutional range of these rights, they apply to companies outside the country, provided that Venezuelan persons or entities domiciled in the country are affected.

Wherever an initiative, whether commercial or not, is addressed at Venezuelan residents, the local courts/agencies can claim jurisdiction, and so it would be advisable to have a local entity acting as representative of the entity responsible for the initiative.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Venezuela?

"Personal information/data" is all information about any individual and/or his/her assets.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

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 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Key privacy principles 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 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

When it comes to advertising, all responsible entities must be sure to:

(a) obtain express consent from the individuals who will be part of the activity; and

(b) post a privacy policy in Spanish.

When it comes to dealing with underage persons, special and mandatory processes must be followed.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Venezuela? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

The Special Law of Cybercrimes establishes a set of sanctions (prison term of between two and six years plus monetary sanctions) for those who breach IT systems, enabling unauthorized access to personal data.

6.2 How are data breaches regulated in Venezuela? What are the requirements for responding to data breaches?

See question 6.1. There is no regulation covering how to respond to such incidents.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Article 60 of the National Constitution 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."

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The Venezuelan law on consumer protection was revoked in 2015, and current legislation does not cover cybersecurity from a consumer rights perspective.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

Not applicable.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Not regulated.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Prior consent and full disclosure is needed.

8.5 Are there specific privacy rules governing data brokers?

No.

8.6 How is social media regulated from a privacy perspective?

Use of social media is only relevant to the current government, when it touches sensitive issues for the government/officers.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Once again, express consent for the use of personal data must be obtained, including approval for sharing such data with third parties.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

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 kind of transactions.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

No.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Violations of privacy or data security law are punishable with prison sentences of between two and seven years, depending on the circumstances, plus monetary sanctions.

10.2 Do individuals have a private right of action? What are the potential remedies?

Yes. Remedies for individuals range from injunctions and suspension of the infringement, up to monetary compensation for moral damages.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Venezuela which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

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 cautions around processing personal information/personal data in Venezuela?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Venezuela has entered the international political agenda for the wrong reasons, and tolerance in Venezuela for criticism is close to none. Diplomatic relationships with several governments, including the USA, are at a historic low, and, for this reason, extreme prudence is advised. However, formally speaking, while legislation does not cover the majority of topics of interest related to data privacy, the fact that it is recognised as a constitutional right can never be ignored.

12.2 What do you envision the privacy landscape will look like in 5 years?

A complete reshape of legal topics of global interest is expected if a political transition begins.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

Uncertainty, due to the lack of regulation on most of the relevant issues associated with data privacy, leaving government officers/judiciary with a wide discretion as to interpretation.

ZIMBABWE

1 PRIVACY LAW

1.1 How is privacy regulated in Zimbabwe?

The Constitution makes provision for the protection of privacy in sections on Right to Privacy and Access to Information.

The Access to Information and Protection of Privacy Act was enacted by Parliament to deal with protection of individuals through 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 government. Private entities are not regulated by this Act.

Although the government has announced its intention to enact legislation to implement the right to privacy, specifically by introduction of a Data Protection Bill, no such legislation has to date been enacted. In the absence of legislation, individuals must rely upon various other laws and the common law to enforce their rights to privacy and data protection in the courts against private entities and individuals.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

Although the Constitution explicitly recognizes the right to privacy, the only specific law enacted related to privacy is the Access to Information Act which, as previously noted, does not apply to private entities and individuals. The missing link is the requisite legislation for the provision in the Constitution of Zimbabwe which guarantees protection. 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, however, do refer to the protection of privacy and information as a function of other activities, or the protection of specific types of rights, such as: the Courts and Adjudicating Authorities (Publicity Restrictions) Act, the Census and Statistics Act, Banking Act, National Registration Act, and the recently enacted Consumer Protection Act.

There is no self-regulatory framework.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Enforcement of rights is through laws related to specific activities or the common law, if applicable, in the courts. There are no self-regulatory bodies.

2 SCOPE

2.1 Which companies are subject to privacy law in Zimbabwe?

The Access to Information Act only covers public bodies; and other Acts which cover specific activities are also aimed at government entities, with exception of consumer protection, banking and healthcare institutions, which are specifically required to avoid disclosure of sensitive information.

There is no specific law on privacy and data protection which imposes obligations on private entities and individuals. The proposed Data Protection legislation has not yet been considered by Parliament. There are, however, laws which provide for limited privacy and data protection, regulating companies in the financial sectors (Banking Act) and retailers of goods and services (Consumer Protection Act).

2.2 Does privacy law in Zimbabwe apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Privacy law in Zimbabwe does not apply to companies outside the country.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Zimbabwe?

The Access to Information Act, which specifically only applies to government agencies, defines "personal information" as recorded information including:

(a) person's name, address or telephone number;

(b) race, national or ethnic origin, colour, religious or political beliefs or associations;

(c) age, sex, sexual orientation, marital status or family status;

(d) identifying number, symbol or other particulars assigned to that person;

(e) fingerprints, blood type or inheritable characteristics;

(f) information about a person's health care history, physical or mental disability;

(g) information about educational, financial, criminal or employment history;

(h) anyone else's opinions about the individual; and

(i) the individual's personal views or opinions.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

Personal information and data related to children, health conditions and financial status are considered sensitive.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

Key privacy principles that companies need to follow are:

(a) avoid disclosure of sensitive information related to health conditions, children and financial status;

(b) where personal data is necessary to know, or limited disclosure required, seek advance written consent.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

There are no specific privacy laws governing companies' processing and use of personal information/personal data. There are some laws requiring confidentiality of personal information, eg, Consumer Protection Act, Banking Act, Labour Act, etc.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

There are no privacy laws imposing obligations on private entities related to the posting of a privacy policy, keeping records of processing operations, etc.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Zimbabwe? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

There are no data or privacy laws governing private entities which regulate or impose minimum standards for securing data, etc.

6.2 How are data breaches regulated in Zimbabwe? What are the requirements for responding to data breaches?

There is currently no specific legislation which provides a remedy to counter data breaches.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

Individuals enjoy privacy rights with respect to their personal information/private data in terms of the Constitution, various laws such as Consumer Protection Law, Banking Law, Labour Law, as well as the common law. The rights may, however, be curtailed for a number of reasons, including law enforcement, national security and related purposes.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

The privacy of individuals remains at stake in Zimbabwe, as marketing communications are circulated without their approval. Through mobile communication providers, companies have a habit of circulating adverts inviting mobile users to participate in gaming Apps from as little as 50c/day and/or encouraging the consumer to subscribe on its website.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

There is currently no law which addresses tracking technologies, although the recently enacted Consumer Protection Act may be interpreted as affording protection to consumers in this area.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There is currently no law which addresses targeted and behavioral advertising from a privacy perspective.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

Under the newly enacted Consumer Protection Act, notice and consent are required in order to share data with third parties for customer matching, but there is no specific type or format specified.

8.5 Are there specific privacy rules governing data brokers?

No. There are no specific privacy rules governing data brokers.

8.6 How is social media regulated from a privacy perspective?

From a privacy perspective, social media is not currently regulated.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs and promotions are not currently regulated.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

The same restrictions related to confidentiality will apply.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

The same restrictions related to confidentiality will apply.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security 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 individuals have a private right of action? What are the potential remedies?

Depending upon the circumstances, there may be a private right of action in court; and damages as well as an interdict may be granted.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Zimbabwe which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The recently enacted Consumer Protection Act and the proposed Data Protection Bill.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Zimbabwe?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/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.

12.2 What do you envision the privacy landscape will look like in 5 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.

12.3 What are some of the 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.

In June 2014, the African Union, to which Zimbabwe is a Member, adopted the African Union Convention on Cyber Security and Personal Data Protection. Chapter II of the Convention sets out the principles and rights which the Member States agree to implement within their jurisdictions.

In August 2016, the Cabinet of the government of Zimbabwe approved the Revised National Policy for Information Communication Technology ("ICT Policy"). According to the approved ICT Policy, the establishment of an institutional framework for enacting legislation dealing specifically with digital data protection and cybersecurity matters is anticipated. In 2018, the Data Protection Bill was announced as part of the legislative agenda. However, it has not, to date, been presented to Parliament of Zimbabwe.

LIST OF GALA MEMBERS

ARGENTINA

Paula Fernandez Pfizenmaier
& Alejandro Massot
Randle Legal
Carlos Pellegrini 1135. 2nd
Buenos Aires B1009ABW
T: +54.11. 5252.0700
E: pfernandez@randlelegal.com
E: amassot@randlelegal.com
W: www.randlelegal.com

AUSTRALIA

Peter Le Guay
Thomson Geer
Level 14, 60 Martin Place
Sydney NSW 2000
T: +61.2.8248.5800
E: pleguay@tglaw.com.au
W: www.tglaw.com.au

AUSTRIA

Stefan Kofler & Georg Huber
Greiter, Pegger, Kofler & Partners
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

Marcos Mercado
Guevara & Gutierrez S.C.
Torre Ketal, Piso 4, Oficina 2 -
Calacoto La Paz
T: +591.2.2770808
E: mmercado@gg-lex.com
W: www.gg-lex.com

BRAZIL

Valdir Rocha
Veirano Advogados
Av. Presidente Wilson, 231, 23. andar
20030-021 - Rio de Janeiro
T: +55.21.38244747
E: valdir.rocha@veirano.com.br
W: www.veirano.com.br

BULGARIA

Kalina Tchakarova & Violetta Kunze
Djingov, Gouginski, Kyutchukov
& Velichkov
10 Tsar Osvoboditel Blvd.
Sofia 1000, Bulgaria
T: +00359.2.932.1105
E: kalina.tchakarova@dgkv.com
E: violetta.kunze@dgkv.com
E: dgkv@dgkv.com
W: www.dgkv.com

CANADA

Kelly Harris & Catherine Dennis Brooks
Miller Thomson LLP
Scotia Plaza, 40 King Street West,
Suite 5800, P.O. Box 1011,
Toronto, Ontario, M5H 3S1
T: 416.595.8582
T: 416.595.8567
E: kharris@millerthomson.com
E: cdennisbrooks@millerthomson.com
W: www.millerthomson.com

CARIBBEAN

Karyl D. Bertrand (Dutch)
Bertrand Legal
Castorweg 22-24
Willemstad, Curaçao
T: +5999 461 8183
E: karyl@bertrand-legal.com

Dianne Daley & Marissa Longsworth
(English)
Foga Daley
7 Stanton Terrace, Kingston 6,
St. Andrew, Jamaica
T: +876 927 4371
E: daley@fogadaley.com
E: marissa@cilglobalip.com
W: www.fogadaley.com

CHILE

Ariela Agosin & Oscar Molina
Albagli Zaliasnik
Av. El Golf 150, Piso 4, Las Condes
Santiago
T: +56 2 2 445 6000
E: aagosin@az.cl
E: omolina@az.cl
W: www.az.cl

CHINA

Justina Zhang
TransAsia Lawyers
1 Jianguomenwai Avenue,
Beijing 100004
T: +86 10 6505 8188
E: whzhang@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.
BLP
BLP Building, 4th floor. Via Lindora
Business Center, San Jose
T: +506.2205.3939
E: uweinstok@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

George Z. Georgiou
George Z. Georgiou & Associates LLC
1 Iras Street, Nicosia 1060
T: +35722763340
E: admin@gzg.com.cy
W: www.gzg.com.cy

CZECH REPUBLIC

Pavel Randl & Irena Lišková
Randl Partners
Budějovická 1550/15a
Praha 4 140 00
T: +420 222 755 311
E: randl@randls.com
E: liskova@randls.com
W: www.randls.com

DENMARK

Johan Løje
Løje IP
Øster Allé 42, 6. floor
P.O.Box 812 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. 27 de Febrero 210
Suite 203 El Vergel
T: +809..373.9418
E: jangeles@angelespons.com
W: www.angelespons.com

ECUADOR

Carlos Alberto Arroyo del Rio
& Jaime Mantilla
Falconi Puig Abogados
Av. Amazonas N21-147 y Roca
Edificio Río Amazonas,
Oficina 900, Quito
T: +593.2. 256.1808
E: carroyo@falconipuig.com
E: jmantilla@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 0000
E: mohamed.eldib@eldib.com
E: dina.eldib@eldib.com
W: www.eldib.com

EL SAVADOR

Marcela Mancia
IDEAS Trademarks & Patents
Séptima calle Poniente Bis y calle José
Martí, 15-229, Colonia Escalón
San Salvador
T: +503.2566.5260
E: mmancia@ideastrademarkslaw.com
W: www.ideastrademarkslaw.com

FINLAND

Mikael Segercrantz &
Johanna Flythström
Roschier, Attorneys Ltd.
Kasarmikatu 21A, Helsinki 00130
T: +503.2566.5260
E: mikael.segercrantz@roschier.com
E: johanna.flythstrom@roschier.com
W: www.roschier.com

FRANCE

Michel Béjot & Caroline Bouvier
Bernard Hertz Béjot
2, rue de Logelbach, Paris 75017
T: +33.1.43.18.8080
E: mbejot@bhbfrance.com
E: cbouvier@bhbfrance.com
W: www.bhbfrance.com

GERMANY

Søren Pietzcker (Hamburg Office),
Dominik Eickemeier (Cologne Office)
& Thorsten Wieland (Frankfurt 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: t.wieland@heuking.de
W: www.heuking.de

GHANA

Olusola Ogundimu
Integrated Legal Consultants
F60/8 Abafun Crescent, Labone, P.M.B.
52, Kanda, Accra
T: +233 302 770 496
E: olusola@integratedlegalconsultants.com
W: www.integratedlegalconsultants.com

GREECE

Kriton Metaxopoulos & Aris I. Syssilas
A. & K. Metaxopoulos & Partners
Law Firm
54 Vas. Sofias Av. , 11528 Athens
T: +30.210.7257614
E: k.metaxopoulos@metaxopouloslaw.gr
E: asyssilas@metaxopouloslaw.gr
W: www.metaxopouloslaw.gr

GUATEMALA

Marco Antonio Palacios &
Hilda Monterroso
Palacios & Asociados / Sercomi
Avenida Reforma 6-64 zona 9
Edificio Plaza Corporativa,
Torre I, Nivel 9,
01009, Guatemala City
T: +502.2385.3416 / 19
E: mapalacios@sercomi.com.gt
E: hmonterroso@sercomi.com.gt
W: www.sercomi.com.gt

HONDURAS

José M. Álvarez & Fernando Godoy
BLP
Torre Nova, 5th Floor, Suite 95-A, Paseo
Los Próceres, Tegucigalpa 11101
T: 504 2269 1217
E: jalvarez@blplegal.com
E: fgodoy@blplegal.com
W: www.blplegal.com

HONG KONG

Angus Forsyth
Angus Forsyth & Co.
16A, Hillier Commercial Building,
65-67 Bonham Strand
Sheung Wan
T: +852.2638.9099
E: angus@angfor.hk
W: www.angfor.hk

HUNGARY

Anikó Keller & Zoltán Kovács
Szecskay Attorneys at Law
H-1055 Budapest, Kossuth Lajos tér 16-17
T: +36 1 472 3000
E: aniko.keller@szecskay.com
E: zoltan.kovacs@szecskay.com
W: www.szecskay.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
Gainsboro House, 24 Suffolk Street, 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.com
W: www.kgcolaw.com

ITALY

Donata Cordone, Laura Liguori & Fabiana Bisceglia
Portolano Cavallo
Piazza Borromeo 12
Milan 20123
T: +39. 02 722 341
E: dcordone@portolano.it
E: lliguori@portolano.it
E: fbisceglia@portolano.it
W: www.portolano.it

JAPAN

Chie Kasahara
Atsumi & Sakai
Fukoku Seimei Bldg., Reception: 12F
2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011
T: +81 3-5501-2438 (Direct)
E: chie.kasahara@aplaw.jp
W: www.aplaw.jp/en/

KENYA

John Syekei & 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: ariana.issaias@bowmanslaw.com
W: www.bowmanslaw.com

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, Level 19 Block 3B,
Plaza Sentral, Jalan Stesen Sentral 5
50470 Kuala Lumpur
T: +603.2278 86 86
E: malaysia@mirandah.com
W: www.mirandah.com

MALTA

Georg Sapiano
Aequitas Legal
Valletta Buildings, South Street
Valletta, 1103
T: +356 21 234085
E: gsapiano@aequitas.com.mt
W: www.aequitas.com.mt

MEXICO

Roberto Arochi, Dafne Méndes & José Antonio Arochi
Arochi & Lindner
Insurgentes Sur 1605, 20th Floor
San José Insurgentes, Mexico City, 03900
T: +52.55.50.95.2050
E: rarochi@arochilindner.com
E: smendez@arochilindner.com
E: jarochi@arochilindner.com
W: www.arochilindner.com

NETHERLANDS

Daniël Haije & Lisanne Steenbergen
Hoogenraad & Haak
Jozef Israelskade 48 G,
Amsterdam 1072 SB
T: +31 20 305 3066
E: dh@hoogenhaak.nl
E: ls@hoogenhaak.nl
W: www.hoogenhaak.nl

NEW ZEALAND

Erich Bachmann & Julika Wahlmann-Smith
Hesketh Henry
Level 14, PwC Tower, 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
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
O. Kayode & Co.
2nd Floor, 21 Olanrewaju Street, Oregun
T: +234 1 291 2412
E: lara@okayode.com
W: www.okayode.com

NORWAY

Bente Holmvang
Bull & Co Advokatfirma AS
Postboks 2583 Solli, N-0203 Oslo
T: +47.23.01.01.01
E: bho@bullco.no
W: www.bullco.no

PANAMA

Ramón R Benedetti A.
Estudio Benedetti
Edificio Comosa, Piso 19,
Avenida Samuel Lewis, Panama 5
T: + 507 321 5700
E: ramon@estudiobenedetti.com
W: www.benedetti.com.pa

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: lilianandolan@mersanlaw.com
W: www.mersanlaw.com

PERU

Jorge Allende, Dafne Ramos
& Magali García
Allende & Garcia Abogados
Av. del Pinar 180 Of. 504,
Chacarilla, Lima 33
T: + 51 1 372 0395
E: jorge@allendegarcia.com.pe
E: dafne@allendegarcia.com.pe
E: magali@allendegarcia.com.pe
W: www.allendegarcia.com.pe

POLAND

Ewa Skrzydlo-Tefelska
Sołtysinski Kawecki & Szlezak
Legal Advisors
ul. Jasna 26, 00-054 Warsaw
T: +48.22.608.70.47
E: ewa.tefelska@skslegal.pl
W: www.skslegal.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

Ana Kusak
Stratulat Albulescu Attorneys at Law
221 27 Ion Brezoianu St.,
ground 5th & 6th Floor, Bog'Art Center,
1st District Bucharest
T: 40.21.316.87.49
E: akusak@saa.ro
W: www.saa.ro

RUSSIA

Irina Anyukhina
ALRUD Law Firm
6 floor, 17 Skakovaya Street,
125040, Moscow
T: +7.495.234.96.92
E: ianyukhina@alrud.com
W: www.alrud.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

Dušan Nitschneider & Peter Marciš
NITSCHNEIDER & PARTNERS
Cintorínska 3/A,
811 08 Bratislava
T: +421 2 2092 1213
E: nitschneider@nitschneider.com
E: marcis@nitschneider.com
W: www.nitschneider.com

SOUTH AFRICA

Kelly Thompson, Jenny Pienaar &
Danie Strachan
Adams & Adams
P O Box 1014, Pretoria, 0001
T: +27 12 432 6000
E: kelly.thompson@adamsadams.com
E: jenny.pienaar@adamsadams.com
E: danie.strachan@adamsadams.com
W: www.adamsadams.com

SPAIN

Ignacio Temiño Ceniceros, Rubén Canales
Quinto & Carolina
Montero Peralta
Abril Abogados
Calle Amador de los Rios,
1 Madrid 28010
T: +34 91 7020331
E: ignaciot@abrilabogados.com
E: rcanales@abrilabogados.com
E: cmontero@abrilabogados.com
W: www.abrilabogados.com

SWEDEN

Erik Ullberg & Tobias Bratt
Wistrand
Box 11920, SE-404 39, Göteborg,
T: + 46 31.771.2100
E: erik.ullberg@wistrand.se
E: tobias.bratt@wistrand.se
W: www.wistrand.se

SWITZERLAND

Dr. Rolf Auf der Maur &
Delia Fehr-Bosshard
VISCHER AG
Schuetzengasse 1, P.O. Box 5090,
CH-8021 Zurich
T: +41 58 211 34 00
E: ram@vischer.com
E: dbosshard@vischer.com
W: www.vischer.com

TRINIDAD AND TOBAGO

Olive Ramchand
Fitzwilliam Stone Furness - Smith & Morgan
48-50 Sackville Street
Port of Spain
T: +868 623 1618
E: oramchand@fitzwilliamstone.com
W: www.fitzwilliamstone.com

TURKEY

Ugur Aktekin & Hande Hançer
Gün + Partners Avukatlık Bürosu
Kore Sehitleri Cad. No: 17,
Zincirlikuyu 34394, Istanbul
T: +90.212.3540000
E: ugur.aktekin@gun.av.tr
E: hande.hancer@gun.av.tr
W: www.gun.av.tr

UGANDA

Paul Asiimwe
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
W: www.sipilawuganda.com

UKRAINE

Oleksandr Padalka
Sayenko Kharenko
10 Muzeyny Provulok,
Kyiv 01001
T: +380 44 499 6000
E: opadalka@sk.ua
W: www.sk.ua

UNITED KINGDOM

Brinsley Dresden
Lewis Silkin LLP
5 Chancery Lane, Clifford's Inn,
London EC4A 1BL
T: +44 (0) 20.7074.8069
E: brinsley.dresden@lewissilkin.com
W: www.lewissilkin.com

UNITED ARAB EMIRATES

Fiona Robertson
Al Tamimi & Company
6th Floor, Building 4 East Dubai
International Financial Centre Sheikh Zayed
Road PO Box 9275 Dubai
T: + 971 (0)4 364 1641
E: f.robertson@tamimi.com
W: www.gun.av.tr

UNITED STATES OF AMERICA

Ronald R. Urbach, Joseph J. Lewczak
& Allison Fitzpatrick
Davis & Gilbert LLP
1740 Broadway,
New York, NY 10019
T: +1.212.468.4800
E: rurbach@dglaw.com
E: jlewczak@dglaw.com
E: afitzpatrick@dglaw.com
W: www.dglaw.com

Daniel Goldberg, Jeffrey A. Greenbaum
& Brian Murphy
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: bmurphy@fkks.com
W: www.fkks.com

Melissa L. Steinman & Angel Garganta
Venable LLP
600 Massachusetts Avenue NW
Washington D.C. 20001
T: + 1 202 344 4000
E: mlsteinman@venable.com
E: agarganta@venable.com
W: www.venable.com

URUGUAY

Agustin Mayer
Ferrere Abogados
Juncal 1392, Ferrere Tower,
11.000 Montevideo
T: +598 2 900 1000
E: amayer@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.com.ve
W: www.antequera.com.ve

ZIMBABWE

Brenda M. Wood Kahari
B.W. Kahari
Baronage House, 24 Lanark Road
Belgravia/Avondale, Harare
T: +263.4.250994/5 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