THE GOVERNMENT PROCUREMENT REVIEW
THE DOMINANCE AND MONOPOLIES REVIEW
THE AVIATION LAW REVIEW
THE FOREIGN INVESTMENT REGULATION REVIEW
THE ASSET TRACING AND RECOVERY REVIEW
THE INSOLVENCY REVIEW
THE OIL AND GAS LAW REVIEW
THE FRANCHISE LAW REVIEW
THE PRODUCT REGULATION AND LIABILITY REVIEW
THE SHIPPING LAW REVIEW
THE ACQUISITION AND LEVERAGED FINANCE REVIEW
THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW
THE PUBLIC–PRIVATE PARTNERSHIP LAW REVIEW
THE TRANSPORT FINANCE LAW REVIEW
THE SECURITIES LITIGATION REVIEW
THE LENDING AND SECURED FINANCE REVIEW
THE INTERNATIONAL TRADE LAW REVIEW
THE SPORTS LAW REVIEW
THE INVESTMENT TREATY ARBITRATION REVIEW
THE GAMBLING LAW REVIEW
THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW
THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW
THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW
THE ISLAMIC FINANCE AND MARKETS LAW REVIEW
THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW
THE CONSUMER FINANCE LAW REVIEW
THE INITIAL PUBLIC OFFERINGS REVIEW
THE CLASS ACTIONS LAW REVIEW
THE TRANSFER PRICING LAW REVIEW
THE BANKING LITIGATION LAW REVIEW
THE HEALTHCARE LAW REVIEW

www.TheLawReviews.co.uk

© 2017 Law Business Research Ltd
ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS
ASTREA
BAKER & MCKENZIE – CIS, LIMITED
BOGSCH & PARTNERS LAW FIRM
DUCLOS, THORNE, MOLLET-VIÉVILLE & ASSOCIÉS (DTMV)
JUN HE LLP
KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J
LEE & KO
M&M BOMCHIL
NNOVATION LLP
PERCHSTONE & GRAEYS
SANTAMARINA Y STETA, SC
SIDLEY AUSTIN LLP
SIQUEIRA CASTRO – ADVOGADOS
SK CHAMBERS
SUBRAMANIAM & ASSOCIATES
URÍA MENÉNDEZ ABOGADOS, SLP
VDA VIEIRA DE ALMEIDA
WALDER WYSS LTD
WINHeller REchtsanwaltsgesellschaft mbH
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Country</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Hong Kong</td>
<td>Yuet Ming Tham</td>
<td>144</td>
</tr>
<tr>
<td>13</td>
<td>Hungary</td>
<td>Tamás Gödölle</td>
<td>159</td>
</tr>
<tr>
<td>14</td>
<td>India</td>
<td>Aditi Subramaniam and Sanuj Das</td>
<td>176</td>
</tr>
<tr>
<td>15</td>
<td>Japan</td>
<td>Tomoki Ishiara</td>
<td>190</td>
</tr>
<tr>
<td>16</td>
<td>Korea</td>
<td>Kwang Bae Park and Ju Bong Jang</td>
<td>206</td>
</tr>
<tr>
<td>17</td>
<td>Malaysia</td>
<td>Shanthi Kandiah</td>
<td>220</td>
</tr>
<tr>
<td>18</td>
<td>Mexico</td>
<td>César G Cruz-Ayala and Diego Acosta-Chin</td>
<td>234</td>
</tr>
<tr>
<td>19</td>
<td>Nigeria</td>
<td>Folabi Kuti, Ugochukwu Obi and Seth Azubuike</td>
<td>247</td>
</tr>
<tr>
<td>20</td>
<td>Poland</td>
<td>Anna Kobylańska and Marcin Lewoszewski</td>
<td>260</td>
</tr>
<tr>
<td>21</td>
<td>Portugal</td>
<td>Magda Cocco and Inês Antas de Barros</td>
<td>272</td>
</tr>
<tr>
<td>22</td>
<td>Russia</td>
<td>Elena Kukushkina, Georgy Mzhavanadze and Vadim Perevalov</td>
<td>284</td>
</tr>
<tr>
<td>23</td>
<td>Singapore</td>
<td>Yuet Ming Tham</td>
<td>296</td>
</tr>
<tr>
<td>24</td>
<td>Spain</td>
<td>Leticia López-Lapuente and Reyes Bermejo Bosch</td>
<td>314</td>
</tr>
<tr>
<td>25</td>
<td>Switzerland</td>
<td>Jürg Schneider, Monique Sturny and Hugh Reeves</td>
<td>327</td>
</tr>
<tr>
<td>Chapter 26</td>
<td>UNITED KINGDOM .................................................................</td>
<td>347</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td></td>
<td>William RM Long, Géraldine Scali and Francesca Blythe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chapter 27</td>
<td>UNITED STATES ..................................................................</td>
<td>364</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alan Charles Raul, Frances E Faircloth and Vivek K Mohan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix 1</td>
<td>ABOUT THE AUTHORS................................................................</td>
<td>393</td>
<td></td>
</tr>
<tr>
<td>Appendix 2</td>
<td>CONTRIBUTING LAW FIRMS’ CONTACT DETAILS.........................</td>
<td>409</td>
<td></td>
</tr>
</tbody>
</table>
For 2017, the world’s principal privacy and data protection issues centred once again on the challenges of transferring personal data between the European Union and the United States. As of October 2017, over 2,500 organisations had already certified compliance with the standards of the transatlantic Privacy Shield. While both sides expect the Privacy Shield to survive the EU’s first annual review of the Privacy Shield’s operation, the fate of this limited ‘adequacy’ decision for the United States will ultimately be decided by the Court of Justice of the European Union (CJEU). This is the same tribunal that previously invalidated the US–EU Safe Harbor Framework in a case brought by Austrian student Max Schrems.

In addition to judging the validity of the Privacy Shield, the CJEU will confront the issue of whether standard contractual clauses (also known as model contracts) can properly be used to transfer data to the United States. This issue was referred to the CJEU by the High Court of Ireland in another case brought by Mr Schrems in his never-ending campaign to prevent any of his social media data from being transferred to the US headquarters of the social media company he prefers to use.

The Privacy Shield, like Safe Harbor before it, concerns only transfers to the United States, and the Irish court case also specifically addressed the viability of model contracts for transfers to the United States. Nonetheless, if the CJEU were to invalidate model contracts, this could in principle disrupt transfers of personal information from the EU to any country whose data protection regime has not yet been deemed ‘adequate’. This could of course put a brake on significant amounts of international trade, investment and business. Furthermore, if the CJEU outcome were negative only with respect to the United States, there would come a point where discrimination and denial of ‘national treatment’ would become a trade issue for the EU and the United States. This could be a problem for the EU, since the checks and balances that each Member State imposes on its own government’s surveillance for national security and law enforcement purposes may not be equivalent to the safeguards imposed by the United States.

In 2017, the EU has also focused intensely on itself. The new General Data Protection Regulation (GDPR), which will enter into effect in May 2018, has captured the fevered attention of businesses inside and outside Europe because of its potential for imposing very significant penalties. Violations could result in payments of €20 million or 4 per cent of global turnover, whichever is higher. Moreover, the GDPR will apply not only to companies established in the EU, but also to those processing data about Europeans if they offer services in the EU or monitor the online activities of individuals located there. It remains to be seen whether the EU and its Member States will develop procedural rules and fairness standards
to ensure that companies accused of violating the GDPR receive due process, as well as an effective 'consistency' mechanism under the new European Data Protection Board. Another question is whether the EU will avoid disproportionately targeting US companies for major penalties or investigations.

The GDPR imposes heightened obligations on companies to obtain consent from the individuals about whom they collect data, and citizens will have powerful rights to object to online profiling, which will have to be advertised in a highly visible manner, and to receive some explanation about significant decisions that affect them that were based on algorithms or automated processes. The consent of parents will also be required for processing information about children under 16, unless individual EU Member States lower the age of consent (but not younger than 13). In general, controllers in the EU will need to focus more intensely on the grounds justifying their collection and processing of data to the extent that they do not have or cannot obtain consent. The scope of 'legitimate interests' of the controller will be a hotly debated topic in the EU for years.

EU residents will also have greater rights to ‘data portability’, which will require companies to collaborate on interoperability. Significantly, this portability right will not exclude data inferred or derived by the controller, and the right is not restricted to data communicated to the company directly by the data subject. Companies will be obligated to undertake privacy impact assessments where they process high-risk data; for example, profiling based on sensitive data such as health information. Where the risk of processing cannot be mitigated by privacy-enhancing measures, the company may need to consult with the relevant data protection authority (DPA). Companies will also need to consider appointing data protection officers (DPOs) for their EU operations, or document why they have concluded that no DPO is necessary. DPOs must be accessible in the EU but are not required to be physically resident there.

The GDPR will also bring mandatory data breach notification to the EU, which will now require DPAs to be notified within 72 hours of a breach, if feasible. Affected individuals must be notified if the breach is likely to result in high risk to them.

The EU is also considering a new ePrivacy Regulation for implementation in 2018 (possibly contemporaneous with the effective date of the GDPR), which will apply to an expanded array of communication services. The EU’s network security directive also goes into effect for Member States in 2018.

In the United States, major data breaches continue to prompt significant litigation, financial settlements and enforcement actions by the Federal Trade Commission (FTC) and state attorneys general. The FTC has also brought significant privacy cases, such as a US$2.2 million settlement negotiated with a TV manufacturer alleged to have been collecting viewing data from users of its televisions without their knowledge. In 2017, the United States appeared to continue to lead the world in privacy enforcement and litigation.

In a case where a tech company announced in 2016 that it experienced breaches affecting 1 billion and 500 million users in 2013 and 2014 respectively, the board of directors conducted an independent investigation that was viewed by many in the legal community as establishing new expectations for the responsibility of general counsels and senior executives to investigate, analyse and escalate data security events.

On the policy front, the US Congress invoked its power to review major regulations by voting to rescind the privacy regulations imposed on internet service providers (ISPs) – but
Global Overview

only ISPs – by the Federal Communications Commission (FCC). President Trump signed the law that invalidated the ISP privacy rules that had been issued by the FCC during the administration of President Obama.

Global developments also tend to confirm continued change, instability and uncertainty in the world of privacy and cybersecurity. In China, a draft, specific data protection law remains under discussion, but the current complicated system of multiple privacy laws remains in place. China continues to debate whether to continue in the direction of a US consumer protection model or to adopt a European one. In the meantime, a 2010 law established tort liability for privacy violations, and the unauthorised sale or acquisition of personal information could be a criminal offence. A Chinese court has held, however, that the use of cookies by ISPs for targeted advertising does not violate the Chinese right of privacy.

China’s major new Cybersecurity Law entered into effect on 1 June 2017. It established a new legal system for protection against cyberthreats and imposed stricter requirements and penalties regarding the cross-border transfer of certain types of data from China. However, implementation provisions are still to be worked out. Data localisation requirements have been imposed on personal information in the banking sector and the country’s new Counter-Terrorism Law requires telecom and internet companies to cooperate more extensively with the government. Like the Cybersecurity Law, the Counter-Terrorism Law’s details and interpretation remain unclear.

In Russia, the 2014 data localisation law requiring primary data processing to be conducted in Russia has forced businesses to modify their practices to comply. Recent counter-terrorism laws have imposed added data retention and government-access burdens on internet businesses. Russia obtained an agreement from Twitter to transfer servers to Russia by the middle of 2018 and an enforcement action against LinkedIn proceeded even though that company had no physical presence in the country. The Russian court rejected LinkedIn’s argument on the grounds that the company was deliberately targeting Russian users in the Russian language.

In India, the country’s Supreme Court declared privacy to be a fundamental constitutional right. As in the EU and the United States, the right to privacy is not absolute, and the Court noted that the right is subject to reasonable restrictions. As in Europe, privacy is deemed to include a right to control data on the internet and the right to be forgotten.

In France, this year’s emphasis has been on the development of additional cybersecurity laws.

Regarding privacy enforcement, a €150,000 penalty was imposed on a social media company for combining data for targeted advertising and tracking allegedly without user knowledge or consent on third-party sites.

In Spain, use may not be made of online behavioural advertising and profiling in reliance on the EU’s ‘legitimate interest’ standard. Thus, express prior consent may be required.

The United Kingdom has stated its intention to adopt a law implementing the GDPR before Brexit occurs.

In Singapore, proposed changes to the country’s data protection act are pending and the passage of significant changes to Singapore’s legal requirements for cybersecurity are believed to be imminent.

Japan adopted major changes to its law in 2016 with a new Privacy Protection Act, which follows an EU model, including an adequacy requirement for transfers to other countries. The new Act implemented drastic changes that entered into force on 30 May 2017. The law also established a new independent enforcement agency.
In Korea, a new law was adopted requiring more conspicuous notice and consent regarding collection and use of personal information. The legislation responded to a court case invalidating consent where the disclosures were made in a font too small for informed consent. In 2017, Korea also became the 21st economy to join the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system.

Despite the government’s efforts, Nigerian hackers are estimated to have stolen US$3 billion worldwide. Privacy is a fundamental right under the country’s constitution and there is some government enforcement in the data protection arena.

In Australia, mandatory data breach reporting goes into effect as of 22 February 2018, with notification required for incidents posing serious harm to individuals.

Argentina is considering the creation of a new autonomous and independent enforcement agency outside the Ministry of Justice and Human Rights. This is believed to be necessary to retain the country’s status as adequate for EU purposes.

In Brazil, privacy is still only regulated in the context of internet use, but new data protection bills are pending. While a court denied a preliminary injunction to enjoin Google’s scanning of emails allegedly without user consent, the litigation remains unresolved.

Mexico enacted a new privacy legal framework on 27 January 2017. A new (or at least newly named) agency has been placed in charge of enforcing the country’s data protection law. The new agency is considered to be an autonomous entity.

Canada, like the EU, is extending its privacy regime extraterritorially. A court has held that the country’s federal privacy law, PIPEDA, applies to organisations that process data about Canadians even if the company is not present in Canada. Mandatory data breach notification is still under discussion but has not been adopted.

The above discussion highlights some of the more notable privacy and cybersecurity developments for 2017 covered in greater detail in the succeeding chapters. There was, of course, also further considerable activity throughout the rest of the world.

* * *

The year ahead is likely to bring increased attention to connected devices, autonomous vehicles, artificial intelligence, machine learning, big-data analytics and predictive algorithms. These novel areas hold serious implications for security (as in hacking cars or medical devices), as well as uncertain and abstract or ethereal impacts on personal autonomy, privacy and profiling. Data transfer disputes, data localisation trends, aggressive government demands for decryption and access to underlying software code and algorithms, election hacking and fake news will roil digital trade and even affect political stability. The intersection of cybersecurity, counter-terrorism, privacy and human rights remains fraught and subject to abuse, hypocrisy and checks and balances in different jurisdictions. The field of privacy, data protection and cybersecurity will thus continue to eschew equilibrium for the foreseeable future.
Chapter 2

EUROPEAN UNION OVERVIEW

William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul

I OVERVIEW

In the EU, data protection is principally governed by the EU Data Protection Directive 95/46/EC (the Data Protection Directive), which regulates the collection and processing of personal data across all sectors of the economy.

The Data Protection Directive has been implemented in all 28 EU Member States through national data protection laws. The reform of EU data protection laws has been the subject of intense discussion following the European Commission’s publication in January 2012 of its proposal for an EU Data Protection Regulation, which would replace the Data Protection Directive and introduce new data protection obligations for data controllers and processors, and new rights for individuals. This proposal was adopted in May 2016 as the EU’s General Data Protection Regulation (the Regulation) and will apply in all Member States from 25 May 2018. The Regulation creates a single EU-wide law on data protection and introduces significant enforcement powers, including fines of up to 4 per cent of annual worldwide turnover or €20 million, whichever is the greater.

In addition, there has also been a significant development in transatlantic data flows with the adoption, on 12 July 2016, of the EU–US Privacy Shield (the Privacy Shield), replacing the now invalidated US–EU Safe Harbor Framework.

Set out in this chapter is a summary of the main provisions in the Data Protection Directive and the Regulation. We then cover guidance provided by the EU’s Article 29 Working Party on the topical issues of cloud computing and whistle-blowing hotlines. We conclude by considering the EU’s Network and Information Security Directive (the NIS Directive).

---

1 William RM Long and Alan Charles Raul are partners, Géraldine Scali is a counsel and Francesca Blythe is an associate at Sidley Austin LLP.
3 Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
4 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
II EU DATA PROTECTION DIRECTIVE

The Data Protection Directive, as implemented into the national data protection laws of each Member State, imposes a number of obligations in relation to the processing of personal data. The Data Protection Directive also provides several rights to data subjects in relation to the processing of their personal data.

Failure to comply with the Data Protection Directive, as implemented in the national laws of EU Member States, can amount to a criminal offence and can result in significant fines and civil claims from data subjects who have suffered as a result.

Although the Data Protection Directive sets out harmonised data protection standards and principles, the way it has been implemented by different Member States can vary significantly, with some requiring that the processing of personal data be notified to the local data protection authority (DPA).

i The scope of the Data Protection Directive

The Data Protection Directive is intended to apply to the processing of personal data wholly or partly by automatic means and to the processing that forms part of a filing system. The Data Protection Directive is not intended to apply to the processing of personal data by an individual in the course of a purely personal or household activity.

The Data Protection Directive, as implemented through national Member State law, only applies when the processing is carried out in the context of an establishment of the controller within the jurisdiction of a Member State, or, where the controller does not have an establishment in a Member State, processes personal data through equipment located in the Member State other than for the sole purpose of transit through that Member State. There are a number of important definitions used in the Data Protection Directive, which include:

- controller: any person who alone or jointly determines the purposes for which personal data is processed;
- data processor: a natural or legal person that processes personal data on behalf of the controller;
- data subject: an individual who is the subject of personal data;
- establishment: a controller that carries out the effective and real exercise of activity through stable arrangements in a Member State;
- filing system: any structured set of personal data that is accessible according to specific criteria, whether centralised or decentralised, such as a filing cabinet containing employee files organised according to their date of joining or their names;
- personal data: data that relate to an individual who is identified or identifiable either directly or indirectly by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In practice, this is a broad definition including anything from someone’s name, address or national insurance number to information about their taste in clothes; and
- processing: any operation or set of operations performed upon personal data, such as collection, recording, organisation, storage, adaptation, alteration, retrieval,

---

7 Recital 19 of the Data Protection Directive.
consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This definition is so broad that it covers practically any activity in relation to personal data.

ii Obligations of controllers under the Data Protection Directive

Notification
Each Member State is obliged to set up a national DPA that controllers may be required to notify before commencing processing. There are instances where some Member States can exempt controllers from this requirement. For example, if the controller has appointed a data protection officer (DPO) who keeps an internal register of processing activities.

Conditions for processing
Controllers may only process personal data if they have satisfied one of six conditions:

a. the data subject in question has consented to the processing;
b. the processing is necessary to enter into or perform a contract with the data subject;
c. the processing is necessary for the pursuit of a legitimate interest of the controller or a third party to whom the personal data are to be disclosed and the rights of the data subject not overridden;
d. the processing is necessary to comply with a legal obligation;
e. the processing is necessary to protect the vital interests of the data subject; or
f. the processing is necessary for the administration of justice or carried out in fulfilment of a public interest function.

Of these conditions, the first three will be most relevant to business. Personal data that relate to a data subject’s race or ethnicity, political life, trade union membership, religious or other similar beliefs, health or sex life (sensitive personal data) can only be processed in more narrowly defined circumstances. The circumstances that will often be most relevant to a business would be where the data subject has explicitly consented to the processing.

Provision of information
Certain information needs to be provided by controllers to data subjects when controllers collect personal data about them, unless the data subjects already have that information. This information includes the identity of the controller (or the controller’s representative), the purposes of the processing and such further information as may be necessary to ensure that the processing is fair (e.g., the categories of personal data, the categories of recipients of the personal data, and the existence of rights of data subjects to access and correct their personal

---

8 Article 18 of the Data Protection Directive.
9 For example, in Germany, the notification requirement does not apply if the data controller has appointed a data protection officer (Section 4d(2) of the Federal Data Protection Act); or if the controller collects, processes or uses personal data for its own persons, and no more than nine employees are employed in collecting, processing or using personal data, and either the data subject has given his or her consent, or the collection, processing or use is needed to create, carry out or terminate a legal obligation or a quasi-legal obligation with the data (Section 4d(3) of the German Federal Data Protection Act).
10 Article 7 of the Data Protection Directive.
11 Article 8 of the Data Protection Directive.
data). In instances where the personal data are not collected by the controller directly from the data subject concerned, the controller is expected to notify this information at the time it collects the personal data or, where a disclosure is envisaged, at the time the personal data are first disclosed. In cases of indirect collection, it may also be possible to avoid providing the required information if to do so would be impossible or involve a disproportionate effort, or if the collection is intended for scientific or historical research or is collection that is mandated by law.

**Treatment of personal data**

In addition to notification and providing information to data subjects as to how their personal data will be processed, controllers must ensure that the personal data they process are adequate, relevant and not excessive for the purposes for which they were collected. In addition, controllers must keep the personal data accurate, up to date and in a form that permits identification of the data subject for no longer than is necessary.

**Security**

The controller will be responsible for ensuring that appropriate technical and organisational measures are in place to protect the personal data. A controller must also choose a data processor providing sufficient guarantees as to the security measures applied by the data processor. A controller must have a written contract with the data processor under which the data processor agrees to only process the personal data on the instructions of the controller and that obliges the data processor to also ensure the same level of security measures as would be expected from the controller.

**Prohibition on transfers outside the EEA**

Controllers may not transfer personal data to countries outside the European Economic Area (EEA) unless the recipient country provides an adequate level of protection for the personal data. The European Commission can make a finding on the adequacy of any particular non-EEA state and Member States are expected to give effect to these findings as necessary in their national laws. So far, the European Commission has made findings of adequacy with respect to Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. The European Commission is also engaged in adequacy talks with Japan and it is widely expected that a finding of adequacy will be made with respect to Japan by early 2018. In addition, the United States previously reached agreement with the European Commission on a set of ‘Safe Harbor’ principles to which organisations in the United States may subscribe to be deemed ‘adequate’ to receive personal data from controllers in the EU. However, in October 2015 this was declared invalid by the Court of Justice of the European Union (CJEU), leading to intense negotiations between US authorities and the European Commission to develop a replacement trans-Atlantic data transfer mechanism.

---

12 Article 10 of the Data Protection Directive.
15 The EEA consists of the 28 EU Member States together with Iceland, Liechtenstein and Norway.
17 The US–EU Safe Harbor Framework was approved in 2000. Details of the Safe Harbor Agreement between the EU and the United States can be found in European Commission Decision 520/2000/EC.
transfer mechanism. Then on 12 July 2016, the Privacy Shield was adopted by the European Commission, with US companies being able to self-certify under the Privacy Shield from 1 August 2016.\(^\text{18}\)

Where transfers are to be made to countries that are not deemed adequate, other exceptions may apply to permit the transfer.\(^\text{19}\) These include where the data subject has unambiguously consented to the transfer and where the transfer is necessary to perform or conclude a contract that the controller has with the data subject or, alternatively, with a third party if the contract is in the data subject’s interests. In addition, the European Commission has approved the EU Model Contract Clauses, standard contractual clauses that may be used by controllers when transferring personal data to non-EEA countries (a model contract). There are two forms of model contract: one where both the data exporter and data importer are controllers; and another where the data exporter is a controller and the data importer is a data processor. Personal data transferred on the basis of a model contract will be presumed to be adequately protected. However, model contracts have been widely criticised as being onerous on the parties. This is because they grant third-party rights to data subjects to enforce the terms of the model contract against the data exporter and data importer, and require the parties to the model contract to give broad warranties and indemnities. The clauses of the model contracts also cannot be varied and model contracts can become impractical where a large number of data transfers need to be covered by numerous model contracts. However, the status of model contracts is currently uncertain, as we understand that the Irish Data Protection Commissioner has recently issued court proceedings to examine the validity of model contracts.

An alternative means of authorising transfers of personal data outside the EEA is the use of binding corporate rules. This approach may be suitable for multinational companies transferring personal data within the same company, or within a group of companies. Under the binding corporate rules approach, the company would adopt a group-wide data protection policy that satisfies certain criteria and, if the rules bind the whole group, then those rules could be approved by EU DPAs as providing adequate data protection for transfers of personal data throughout the group. The Article 29 Working Party, which is composed of representatives of each Member State and advises the European Commission


\(^{19}\) Article 26 of the Data Protection Directive.
European Union Overview

on data protection matters, has published various documents\textsuperscript{20} on binding corporate rules, including a model checklist for approval of binding corporate rules\textsuperscript{21} and a table setting out the elements and principles to be found in binding corporate rules.\textsuperscript{22}

iii Marketing

The EU Electronic Communications (Data Protection and Privacy) Directive 2002/58/EC (the ePrivacy Directive) places requirements on Member States in relation to the use of personal data for direct marketing. Direct marketing for these purposes includes unsolicited faxes, or making unsolicited telephone calls through the use of automated calling machines, or direct marketing by email. In such instances, the direct marketer needs to have the prior consent of the recipient (i.e., consent on an opt-in basis). However, in the case of emails, there are limited exceptions for email marketing to existing customers where, if certain conditions\textsuperscript{23} are satisfied, unsolicited emails can still be sent without prior consent. In other instances of unsolicited communications, it is left up to each Member State to decide whether such communications will require the recipient’s prior consent or can be sent without prior consent unless recipients have indicated that they do not wish to receive such communications (i.e., consent on an opt-out basis).

The ePrivacy Directive imposes requirements on providers of publicly available electronic communication services to put in place appropriate security measures and to notify certain security breaches in relation to personal data. The ePrivacy Directive was also amended in 2009\textsuperscript{24} to require that website operators obtain the informed consent of users to collect personal data of users through website ‘cookies’ or similar technologies used for storing information. There are two exemptions to the requirement to obtain consent before using cookies: when the cookie is used for the sole purpose of carrying out the transmission

---


WP 195 – Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules adopted on 6 June 2012.

WP 195a – Recommendation 1/2012 on the standard application form for approval of Binding Corporate Rules for the transfer of personal data for processing activities adopted on 17 September 2012.


WP 153 – Working Document setting up a table with the elements and principles to be found in binding corporate rules adopted on 24 June 2008.

\textsuperscript{22} Unsolicited emails may be sent without prior consent to existing customers if the contact details of the customer have been obtained in the context of a sale of a product or a service and the unsolicited email is for similar products or services; and if the customer has been given an opportunity to object, free of charge in an easy manner, to such use of his or her electronic contact details when they are collected and on the occasion of each message in the event the customer has not initially refused such use – Article 13(2) of the ePrivacy Directive.

\textsuperscript{23} Directive 2009/56/EC.

© 2017 Law Business Research Ltd
of a communication over an electronic communications network; and when the cookie is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service.25

The Article 29 Working Party has published an opinion on the cookie consent exemption26 that provides an explanation on which cookies require the consent of website users (e.g., social plug-in tracking cookies, third-party advertising cookies used for behavioural advertising, analytics) and those that fall within the scope of the exemption (e.g., authentication cookies, multimedia player session cookies and cookies used to detect repeated failed login attempts). Guidance on how to obtain consent has been published at a national level by various data protection authorities.27

In July 2016, following the adoption of the Regulation, the Article 29 Working Party issued an opinion on a revision of the rules contained in the ePrivacy Directive.28

On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace the existing ePrivacy Directive.29 The ePrivacy Regulation will complement the Regulation and provide additional sector-specific rules, including in relation to marketing and the use of website cookies.

The key changes in the proposed ePrivacy Regulation will:

a require a clear affirmative action to consent to cookies;

b attempt to encourage the shifting of the burden of obtaining consent for cookie use to website browsers; and

c ensure that consent for direct marketing will be harder to obtain and must meet the standard set out in the Regulation; however, existing exceptions, such as the exemption where there is an existing relationship and similar products and services are being marketed, are likely to be retained.

The European Commission’s original timetable for the ePrivacy Regulation was for it to apply from 25 May 2018 and coincide with the Regulation. However, it is increasingly unlikely that this deadline will be met, both because the ePrivacy Regulation is tied to a wider reform of EU telecommunications regulation and also because of the number of issues with the proposal that have been identified.

In April 2017, the Article 29 Working Party issued an opinion on the proposed ePrivacy Regulation, which welcomed some elements of the proposal but also identified areas of ‘grave concern’, including with regard to cookie tracking walls.30

25 Article 5(3) of the ePrivacy Directive.
26 WP 194 – Opinion 04/2012 on Cookie Consent Exemption.
iv Rights of data subjects under the Data Protection Directive

Data subjects have a right to obtain access to personal data held about them and also to be able to ask for the personal data to be corrected where the personal data is inaccurate.\(^{31}\)

Data subjects also have rights to object to certain types of processing where there are compelling legitimate grounds;\(^{32}\) for example, where the processing would cause the data subject unwarranted harm. Data subjects may also object to direct marketing and to decisions that significantly affect them being made solely on the basis of automated processing.

In May 2014, the CJEU issued a judgment against Google Inc and Google Spain SL in which it ruled that in certain circumstances, search engines are obliged to remove links displayed following a search made on the basis of a person’s name, where the data is incomplete or inaccurate, even if the publication itself on those web pages is lawful. This is based on existing rights under the EU Data Protection Directive to rectification, erasure or blocking of personal data where the individual objects to the processing of the data for compelling legitimate grounds, where the data is inadequate, irrelevant or inaccurate, or excessive in relation to the purposes of the processing, and where the impact on an individual’s privacy is greater than the public’s right to find the data. As of May 2015, Google had received over 253,000 removal requests and had removed approximately 380,000 links from search results.\(^{33}\)

III EU DATA PROTECTION REGULATION

The proposal for the General Data Protection Regulation (the Regulation) was published by the European Commission in January 2012 and has been described as the most lobbied piece of European legislation in history, receiving over 4,000 amendments in opinions from committees in the European Parliament as well as from numerous industries. In March 2014, the European Parliament’s Civil Liberties Committee after several delays finally voted on the European Commission’s proposed EU General Data Protection Regulation and adopted all amendments. Over a year later, in June 2015, the Council of Ministers (which represents EU Member States) published its compromise proposal for the Regulation. This in turn, triggered the commencement of the ‘trilogue’ process – the final stage of negotiations between the three EU institutions. In May 2016, after almost four years of intense negotiations, the Regulation was adopted by the European Parliament at second reading. The Regulation will apply in Member States from 25 May 2018.

The Regulation as adopted will have a significant impact on many governments, businesses and individuals both in and outside the EU. The main elements of the Regulation are summarised below.

---

31 Article 12 of the Data Protection Directive.
33 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and María Costeja González, Case C-131/12.
### Enforcement

The Regulation provides for substantial penalties in the form of administrative fines from DPAs.\(^{34}\) This is an area that underwent much negotiation and change throughout the various stages of negotiation of the Regulation.

As adopted, the Regulation provides a two-tier structure for fines. Functional, operational or administrative infringements of the Regulation will result in fines of up to €10 million or 2 per cent of annual turnover, whichever is the greater, whereas intentional or negligent infringements, or infringements that involve multiple provisions of the Regulation, will be subject to higher fines of up to €20 million or 4 per cent of annual turnover, whichever is the greater. In addition, the Regulation grants data subjects the right to claim damages for non-financial losses, such as distress. These extensive penalties represent a significant change in the field of data protection that should ensure that businesses and governments take data protection compliance seriously.\(^{35}\)

### Scope of the Regulation

The Regulation will apply to the processing of personal data in the context of the activities of a data controller or a processor in the EU and to a controller or processor not established in the EU where the processing activities are related to the offering of goods or services to EU citizens, or the monitoring of such individuals. This means that many non-EU companies that have EU customers will now need to comply with the Regulation.\(^{36}\)

### One-stop shop

The Regulation proposes a new regulatory ‘one-stop shop’ for data controllers that operate in several EU countries. The DPA where the controller is established will be the lead DPA, which must consult with other DPAs before taking action.\(^{37}\) The Article 29 Working Party has adopted guidelines with FAQs on how to identify a controller’s or processor’s lead DPA.\(^{38}\) The guidelines make it clear that the Regulation does not permit ‘forum shopping’ by controllers and processors. In the case of a dispute between DPAs, action can be decided upon by the European Data Protection Board. The Regulation also promotes cooperation among DPAs by requiring the lead DPA to submit a draft decision on a case to the concerned DPAs, on which they will have to reach a consensus prior to finalising any decision.\(^{39}\)

### Profiling

Significantly for online companies, under the Regulation, every individual will now have a general right to object to profiling. In addition, the Regulation imposes a new requirement to inform individuals about the right to object to profiling in a highly visible manner. Profiling that significantly affects the interests of an individual can only be carried out under limited circumstances, such as with the individual’s consent, and should not be automated

---

\(^{34}\) As of September 2017, no significant guidance has been published regarding administrative fines and other penalties under the Regulation.

\(^{35}\) Article 83 of the Regulation.

\(^{36}\) Article 3 of the Regulation.

\(^{37}\) Article 56 of the Regulation.

\(^{38}\) WP 244 – Guidelines for identifying a controller or processor’s lead supervisory authority, adopted on 13 December 2016 and revised on 5 April 2017.

\(^{39}\) Article 60 of the Regulation.
but involve human assessment. These provisions will have a major impact on how online companies market their products and services, and on how many organisations engage in, for example, big-data analytics. Businesses should review their current profiling activities and determine whether these should be modified to ensure compliance with the Regulation.\(^{40}\)

\textbf{v Consent}

Under the Regulation, consent must be informed and freely given, which means that a data subject must have a genuine choice as to whether to consent or not. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations.\(^{41}\) Unlike under the Directive, controllers and processors cannot rely on implied or opt-out consent, and consent should be given by a clear, affirmative act, which may include, for example, ticking a box on a website.\(^{42}\) In addition, it should also be as easy to withdraw consent as it is to give it, with consent being invalid where given for unspecified data processing.\(^{43}\) Processing data on children under the age of 16 also requires the consent of the parent or legal guardian. Member States are entitled to set a lower age provided it is not below the age of 13.\(^{44}\) Companies also cannot make the execution of a contract or a provision of a service conditional upon the receipt of consent from users to process their data.

\textbf{vi Standardised information policies}

The Regulation requires that data subjects be provided with extensive information relating to the processing of their personal data, including being informed about how their personal data will be processed and their rights of access to data, rectification and erasure of data and of the right to object to profiling as well as to lodge a complaint with a DPA and to bring legal proceedings.\(^{45}\) In addition, the Regulation empowers the European Commission to adopt delegated acts for the purpose of providing certain information as standardised icons, as well as the procedures for providing such icons.\(^{46}\)

\textbf{vii Right of erasure}

The ‘right of erasure’ (formerly the ‘right to be forgotten’) gives individuals a right to have their personal data erased where the data are no longer necessary or where they withdraw consent, although a limited number of exemptions also apply, such as where data are required for scientific research or for compliance with a legal obligation of EU law.\(^{47}\)

\textbf{viii Right to data portability}

The right to data portability gives the data subject the right to have their personal data transferred from one controller to another without hindrance when the data are processed in a machine-readable, structured and commonly used format and the legal basis for the

\(^{40}\) Article 22 of the Regulation.
\(^{41}\) Recital 43 of the Regulation.
\(^{42}\) Recital 32 of the Regulation.
\(^{43}\) Article 7 of the Regulation.
\(^{44}\) Article 8 of the Regulation.
\(^{45}\) Article 12 of the Regulation.
\(^{46}\) Article 12(8) of the Regulation.
\(^{47}\) Article 17 of the Regulation.
processing is consent or the performance of a contract with the data subject. This right would, for example, permit a user to have a social media provider transfer his or her personal data to another social media provider.

The Article 29 Working Party has published guidance on the implementation, interpretation and scope of this right. These guidelines recommend that data controllers begin developing technical tools to deal with data portability requests and that industry stakeholders should collaborate to deliver a set of interoperable standards and formats to deliver the right to data portability. The guidelines also clarify which types of personal data the right to data portability should apply to, specifically:

a. that the right applies to data provided by the data subject, whether actively and knowingly (e.g., in a data capture form) or by virtue of the use of a device or service (e.g., search history or location data);

b. the right does not apply to data inferred or derived by the controller from raw data provided by the data subject (e.g., a credit score); and

c. the right is not restricted to data communicated by the data subject directly.

ix Accountability

Controllers will be required to adopt all reasonable steps to implement compliance procedures and policies that respect the choices of individuals, which should be reviewed regularly. Importantly, controllers will need to implement privacy by design and default throughout the life cycle of processing from collection of the data to their deletion. In addition, businesses will need to keep detailed documentation of the data being processed and carry out a privacy impact assessment where the processing uses new technologies and is likely to result in a high risk for individuals, such as profiling or processing sensitive data (e.g., health data) on a large scale. This assessment also has to be reviewed regularly and should be carried out for each new processing system or at least when there is a change in the risk represented by the processing operations. Where a controller has identified a high risk to the individuals that cannot be mitigated through privacy-enhancing measures, that controller should consult with the data protection authority before proceeding with the processing. In April 2017 the Article 29 Working Party published draft guidance on privacy impact assessments. The guidance provided clarification on when controllers must carry out a privacy impact assessment, the methodology they should use, how they should record it and the process for consulting with a data protection authority if residual high risks cannot be mitigated.

x Data protection officers

The Regulation introduces the requirement for controllers and processors to appoint a DPO where the processing is carried out by a public authority; the core activities require regular and systematic monitoring of data subjects on a large scale; or the core activities consist of processing sensitive personal data on a large scale.
Where required to appoint a DPO, the Regulation states that a group of companies can appoint a single DPO provided that he or she is easily accessible from each group company. In addition, there is no requirement to appoint an employee: a third party can be appointed instead. Although the Regulation does not set specific requirements in terms of the level of qualification required, the DPO must have expert knowledge of data protection law and practices and be able to fulfil a prescribed list of tasks. These tasks must be carried out independently and the DPO must report to the highest level of management.

The Article 29 Working Party has published guidelines on the appointment of a DPO. These guidelines indicate that many businesses will not be required to appoint a mandatory DPO, but even where a business believes it is not required to have a mandatory DPO, it should still document the internal analysis that determined whether a DPO was required. The guidelines also detail the level of expertise that a DPO should have and the resources that they should be provided with. It is not a requirement that DPOs must be based in the EEA. However, DPOs must be easily accessible from each establishment.

xi  Security and security breaches
The controller and the processor will need to implement appropriate technical and organisational security measures to ensure a level of security appropriate to the risk. The Regulation also requires that security policies contain a number of elements to ensure appropriate security measures are in place, including, for example, a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.\(^{54}\) In addition, security breaches will need to be notified to DPAs without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Affected individuals will also need to be notified without undue delay where the personal data breach is likely to result in a high risk to their rights and freedoms unless measures are taken to minimise the risk, such as data being encrypted.\(^{55}\)

xii  International data transfers
In addition to binding corporate rules and other data transfer solutions, new methods allowing for international data transfers of personal data from the EU include the use of approved codes of conduct or certification mechanisms. The Regulation also permits such international transfers where they are necessary for the ‘legitimate interests’ of the controller, providing the transfers are not large scale or frequent, the controller has adduced appropriate safeguards and the interests of the affected individuals are not overridden. This form of transfer is only to be used as a last resort and organisations must inform the DPA and data subjects of its reliance on this mechanism.\(^{56}\)

The Regulation also provides a mechanism that restricts Member States from enforcing a judgment issued by non-EU courts or authorities, unless the request is based on an international transfer agreement between that third country and the EU Member State.

---

\(^{53}\) WP 243 – Guidelines on Data Protection Officers ('DPOs') adopted on 13 December and revised on 5 April 2017.

\(^{54}\) Article 32 of the Regulation.

\(^{55}\) Article 33 of the Regulation.

\(^{56}\) Articles 44–48 of the Regulation.
Health data
The Regulation also contains important provisions relating to the use of health data, including the processing of personal data for scientific research that, according to the Regulation, should be considered a compatible form of processing. This provision is important, as it may assist in allowing growth in scientific research for secondary research purposes where existing laws did not.57

IV CLOUD COMPUTING
In its guidance on cloud computing adopted on 1 July 2012,58 the EU’s Article 29 Working Party states that the majority of data protection risks can be divided into two main categories: lack of control over the data; and insufficient information regarding the processing operation itself. The lawfulness of the processing of personal data in the cloud depends on adherence to the principles of the EU Data Protection Directive, which are considered in the Article 29 Working Party Opinion, and some of which are summarised below. It would be reasonable to expect that the Article 29 Working Party will issue new guidance on cloud computing and data protection to reflect new requirements under the Regulation.

i Instructions of the data controller
To comply with the requirements of the EU Data Protection Directive, the Article 29 Working Party Opinion provides that the extent of the instructions should be detailed in the relevant cloud computing agreement (the cloud agreement) along with service levels and financial penalties on the provider for non-compliance.

ii Purpose specification and limitation requirement59
Under Article 6(b) of the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. To address this requirement, the agreement between the cloud provider and the client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or subcontractors.

iii Security60
Under the Data Protection Directive, a data controller must have in place adequate organisational and technical security measures to protect personal data and should be able to demonstrate accountability. The Article 29 Working Party Opinion comments on this point, reiterating that it is of great importance that concrete technical and organisational measures are specified in the cloud agreement, such as availability, confidentiality, integrity, isolation and portability. As a consequence, the agreement with the cloud provider should contain a provision to ensure that the cloud provider and its subcontractors comply with the security measures imposed by the client. It should also contain a section regarding the assessment of

57 Article 9 of the Regulation.
59 Article 6(b) of the Data Protection Directive.
60 Article 17(2) of the Data Protection Directive.
the security measures of the cloud provider. The agreement should also contain an obligation for the cloud provider to inform the client of any security event. The client should also be able to assess the security measures put in place by the cloud provider.

iv Subcontractors
The Article 29 Working Party Opinion indicates that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard, with the controller retaining at all times the possibility to object to the changes or to terminate the agreement. There should also be a clear obligation on the cloud provider to name all the subcontractors commissioned, as well as the location of all data centres where the client’s data can be hosted. It must also be guaranteed that both the cloud provider and all the subcontractors shall act only on instructions from the client. The agreement should also set out the obligation on the part of the processor to deal with international transfers, for example by signing contracts with sub-processors, based on the EU Model Contract Clauses.

v Erasure of data\textsuperscript{61}
The Article 29 Working Party Opinion states that specifications on the conditions for returning the personal data or destroying the data once the service is concluded should be contained in the agreement. It also states that data processors must ensure that personal data are erased securely at the request of the client.

vi Data subjects’ rights\textsuperscript{62}
According to the Article 29 Working Party Opinion, the agreement should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subjects’ rights to access, correct or delete their data, and to ensure that the same holds true for the relation to any subcontractor.

vii International transfers\textsuperscript{63}
As discussed above, under Articles 25 and 26 of the Data Protection Directive, personal data can only be transferred to countries located outside the EEA if the country provides an adequate level of protection.

viii Confidentiality
The Article 29 Working Party Opinion recommends that an agreement with the cloud provider should contain confidentiality wording that is binding both upon the cloud provider and any of its employees who may be able to access the data.

\textsuperscript{61} Article 6 (e) of Data Protection Directive.
\textsuperscript{62} Article 12 and 14 of the Data Protection Directive.
\textsuperscript{63} Article 25 and 26 of the Data Protection Directive.
ix  Request for disclosure of personal data by a law enforcement authority
Under the Article 29 Working Party Opinion, the client should be notified about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as under a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

x  Changes concerning the cloud services
The Article 29 Working Party recommends that the agreement with the cloud provider should contain a provision stating that the cloud provider must inform the client about relevant changes concerning the cloud service concerned, such as the implementation of additional functions.

Once the Regulation takes effect on 25 May 2018, clients and cloud service providers will need to be mindful that references to the Data Protection Directive in the Article 29 Working Party Opinion will be defunct and that the equivalent principles and requirements in the Regulation should be complied with instead. For example, under Article 28(3) of the Regulation, processing by the processor (i.e., the cloud service provider) must be governed by a contract with the controller that stipulates a number of obligations set out by the Regulation.

V  WHISTLE-BLOWING HOTLINES
The Article 29 Working Party published an Opinion in 2006 on the application of the EU data protection rules to whistle-blowing hotlines providing various recommendations, which are summarised below.

i  Legitimacy of whistle-blowing schemes
Under the Data Protection Directive, personal data must be processed fairly and lawfully. For a whistle-blowing scheme, this means that the processing of personal data must be on the basis of at least one of certain grounds, the most relevant of which include where:

a  the processing is necessary for compliance with a legal obligation to which the data controller is subject, which could arguably include a company’s obligation to comply with the provisions of the US Sarbanes-Oxley Act (SOX). However, the Article 29 Working Party concluded that an obligation imposed by a foreign statute, such as SOX, does not qualify as a legal obligation that would legitimise the data processing in the EU; or

b  the processing is necessary for the purposes of the legitimate interests pursued by the data controller, or by the third party or parties to whom the data are disclosed, except where those interests are overridden by the interests or the fundamental rights and freedoms of the data subject. The Article 29 Working Party acknowledged that whistle-blowing schemes adopted to ensure the stability of financial markets, and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting as well as the fight against bribery,

64  WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.
banking and financial crime, or insider trading, might be seen as serving a legitimate interest of a company that would justify the processing of personal data by means of such schemes.

ii Limiting the number of persons eligible to use the hotline
Applying the proportionality principle, the Article 29 Working Party recommends that the company responsible for the whistle-blowing reporting programme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct and the number of persons who might be incriminated. However, the recommendations acknowledged that in both cases the categories of personnel involved may still sometimes include all employees in the fields of accounting, auditing and financial services.

iii Promotion of identified reports
The Article 29 Working Party pointed out that, although in many cases anonymous reporting is a desirable option, where possible, whistle-blowing schemes should be designed in such a way that they do not encourage anonymous reporting. Rather, the helpline should obtain the contact details of reports and maintain the confidentiality of that information within the company, for those who have a specific need to know the relevant information. The Article 29 Working Party also suggested that only reports that included information identifying the whistle-blower would be considered as satisfying the essential requirement that personal data should only be processed ‘fairly’.

iv Proportionality and accuracy of data collected
Companies should clearly define the type of information to be disclosed through the system by limiting the information to accounting, internal accounting control or auditing, or banking and financial crime and anti-bribery. The personal data should be limited to data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

v Compliance with data-retention periods
According to the Article 29 Working Party, personal data processed by a whistle-blowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report. These periods would be different when legal proceedings or disciplinary measures are initiated. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Personal data found to be unsubstantiated should be deleted without delay.

vi Provision of clear and complete information about the whistle-blowing programme
Companies as data controllers must provide information to employees about the existence, purpose and operation of the whistle-blowing programme, the recipients of the reports and the right of access, rectification and erasure for reported persons. Users should also be informed that the identity of the whistle-blower shall be kept confidential, that abuse of the system may result in action against the perpetrator of that abuse and that they will not face any sanctions if they use the system in good faith.
vii Rights of the incriminated person

The Article 29 Working Party noted that it was essential to balance the rights of the incriminated person and of the whistle-blower and the company's legitimate investigative needs. In accordance with the Data Protection Directive, an accused person should be informed by the person in charge of the ethics reporting programme as soon as practicably possible after the ethics report implicating them is received. The implicated employee should be informed about:

a the entity responsible for the ethics reporting programme;
b the acts of which he or she is accused;
c the departments or services that might receive the report within the company or in other entities or companies of the corporate group; and
d how to exercise his or her rights of access and rectification.

Where there is a substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather evidence, then notification to the incriminated person may be delayed as long as the risk exists.

The whistle-blowing scheme also needs to ensure compliance with the individual's right, under the Data Protection Directive, of access to personal data on them and their right to rectify incorrect, incomplete or outdated data. However, the exercise of these rights may be restricted to protect the rights of others involved in the scheme and under no circumstances can the accused person obtain information about the identity of the whistle-blower, except where the whistle-blower maliciously makes a false statement.

viii Security

The company responsible for the whistle-blowing scheme must take all reasonable technical and organisational precautions to preserve the security of the data and to protect against accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. Where the whistle-blowing scheme is run by an external service provider, the EU data controller needs to have in place a data processing agreement and must take all appropriate measures to guarantee the security of the information processed throughout the whole process and commit themselves to complying with the data protection principles.

ix Management of whistle-blowing hotlines

A whistle-blowing scheme needs to carefully consider how reports are to be collected and handled with a specific organisation set up to handle the whistle-blower's reports and lead the investigation. This organisation must be composed of specifically trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations. The whistle-blowing system should be strictly separated from other departments of the company, such as human resources.

x Data transfers from the EEA

The Article 29 Working Party believes that groups should deal with reports locally in one EEA state rather than automatically share all the information with other group companies. However, data may be communicated within the group if the communication is necessary for the investigation, depending on the nature or seriousness of the reported misconduct or results from how the group is set up. The communication will be considered necessary,
for example, if the report incriminates another legal entity within the group involving a high-level member of management of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient entity, which provides equivalent guarantees as regards management of the whistle-blowing reports as the EU organisation.

VI E-DISCOVERY

The Article 29 Working Party has published a working document providing guidance to data controllers in dealing with requests to transfer personal data to other jurisdictions outside the EEA for use in civil litigation to help them to reconcile the demands of a litigation process in a foreign jurisdiction with the data protection obligations of the Data Protection Directive.

The main suggestions and guidelines include the following:

a. Possible legal bases for processing personal data as part of a pretrial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the Article 29 Working Party states that an obligation imposed by a foreign statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. A third possible basis is a legitimate interest pursued by the data controller or by the third party to whom the data are disclosed where the legitimate interests are not overridden by the fundamental rights and freedoms of the data subjects. This involves a balance-of-interest test taking into account issues of proportionality, the relevance of the personal data to litigation and the consequences for the data subject.

b. Restricting the disclosure of data if possible to anonymised or redacted data as an initial step and after culling the irrelevant data, disclosing a limited set of personal data as a second step.

c. Notifying individuals in advance of the possible use of their data for litigation purposes and, where the personal data is actually processed for litigation, notifying the data subject of the identity of the recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

d. Where the non-EEA country to which the data will be sent does not provide an adequate level of data protection, and where the transfer is likely to be a single transfer of all relevant information, then there would be a possible ground that the transfer is necessary for the establishment, exercise or defence of a legal claim. Where a significant amount of data is to be transferred, the Article 29 Working Party previously suggested the use of binding corporate rules or the Safe Harbor regime. However, Safe Harbor was found to be invalid by the CJEU in 2015. The Safe Harbor regime was, however, effectively replaced on 12 July 2016 by the Privacy Shield. In the absence of any updates from the Article 29 Working Party to its e-discovery working document, it can be assumed that the use of Privacy Shield is also an appropriate means of transferring significant amounts of data. It also recognises that compliance with a request made under the Hague Convention would provide a formal basis for the transfer of the data.

---

VII EU CYBERSECURITY STRATEGY

In March 2014, the European Parliament adopted a proposal for the NIS Directive,\(^66\) which was proposed by the European Commission in 2013. The NIS Directive is part of the European Union's Cybersecurity Strategy aimed at tackling network and information security incidents and risks across the EU and was adopted on 6 June 2016 by the European Parliament at second reading.\(^67\)

The main elements of the NIS Directive include:

\(a\) new requirements for 'operators of essential service' and 'digital service providers';
\(b\) a new national strategy;
\(c\) designation of a national competent authority; and
\(d\) designation of computer security incident response teams (CSIRTs) and a cooperation network.

i New national strategy

The NIS Directive requires Member States to adopt a national strategy setting out concrete policy and regulatory measures to maintain a high level of network and information security.\(^68\) This includes having research and development plans in place or a risk assessment plan to identify risks, designating a national competent authority that will be responsible for monitoring compliance with the NIS Directive and receiving any information security incident notifications,\(^69\) and setting up of at least one CSIRT that is responsible for handling risks and incidents.\(^70\)

ii Cooperation network

The competent authorities in EU Member States, the European Commission and the European Union Agency for Network and Information Security will form a cooperation network to coordinate against risks and incidents affecting network and information systems.\(^71\) The cooperation network will exchange information between authorities and also provide early warnings on information security risks and incidents, and agree on a coordinated response in accordance with an EU–NIS cyber-cooperation plan.

iii Security requirements

A key element of the NIS Directive is that Member States must ensure public bodies and certain market operators\(^72\) take appropriate technical and organisational measures to manage the security risks to networks and information systems, and to guarantee a level of security.

---

\(^{66}\) Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013.

\(^{67}\) Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

\(^{68}\) Article 7 of the NIS Directive.

\(^{69}\) Article 8 of the NIS Directive.

\(^{70}\) Article 9 of the NIS Directive.

\(^{71}\) Article 11 of the NIS Directive.

\(^{72}\) Operators of essential services are listed in Annex II of the NIS Directive and include operators in energy and transport, financial market infrastructures, banking, operators in the production and supply of water, the health sector and digital infrastructure. Digital service providers (e.g., e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores) are
appropriate to the risks.\textsuperscript{73} The measures should prevent and minimise the impact of security incidents affecting the core services they provide. Public bodies and market operators must also notify the competent authority of incidents having a significant impact on the continuity of the core services they provide, and the competent authority may decide to inform the public of the incident. The significance of the disruptive incident should take into account:

\begin{itemize}
\item[a] the number of users affected;
\item[b] the dependency of other key market operators on the service provided by the entity;
\item[c] the duration of the incident;
\item[d] the geographic spread of the area affected by the incident;
\item[e] the market share of the entity; and
\item[f] the importance of the entity for maintaining a sufficient level of service, taking into account the availability of alternative means for the provisions of that service.
\end{itemize}

Member States have until May 2018 to implement the NIS Directive into their national laws. Some Member States, such as the United Kingdom, have already started to consult on how they intend to implement the NIS Directive into their national laws.\textsuperscript{74}

\section*{VIII OUTLOOK}

The past 12 months have seen a number of key developments in the European data protection world. The Article 29 Working Party and Member States have begun to issue guidance on aspects of the Regulation. Further guidance from the Article 29 Working Party is expected before the end of 2017 on administrative fines, certifications, profiling, consent, transparency, the notification of personal data breaches and international transfer tools. These guidance documents, together with those published by Member State data protection authorities should provide businesses with a clearer sense of how to comply with the Regulation in practice.

In addition, US companies have been able to self-certify under the Privacy Shield since 1 August 2016. As expected, the Privacy Shield has faced numerous challenges in 2017 from data privacy activists, the actions of the US government and Members of the European Parliament. On 6 April 2017, the European Parliament adopted a resolution stating that deficiencies in the Privacy Shield must be fixed urgently. The European Parliament focused in particular on recent surveillance activities in the United States and the Privacy Shield Ombudsperson mechanism set up by the US Department of State. Another threat to the Privacy Shield is from two legal challenges filed at the CJEU by Digital Rights Ireland and the French advocacy group La Quadrature du Net respectively.\textsuperscript{75} These cases were both filed in the autumn of 2016 and the CJEU is yet to issue a decision in either case. Finally, the European Commission’s inaugural annual review of the Privacy Shield took place in September 2017. This review was conducted jointly by EU and US officials and there was political pressure on the EU to ensure that the review thoroughly examined the shortcomings and weaknesses listed in Annex III. The requirements for digital service providers are less onerous than those imposed on operators of essential services; however, they are still required to report security incidents that have a significant impact on the service they offer in the EU.

\textsuperscript{73} Article 14 of the proposed NIS Directive.

\textsuperscript{74} Security of Network and Information Systems Public Consultation, August 2017.

\textsuperscript{75} Digital Rights Ireland v. Commission, Case T-670/16 and La Quadrature du Net and Others v. Commission, Case T-738/16.
of the Privacy Shield. On 21 September 2017, Commissioner Jourová and the US Secretary of Commerce issued a joint statement indicating that both the EU and the United States remained committed to the continued functioning of the Privacy Shield.

Other mechanisms of transfer, including model contracts, are also facing scrutiny and this raises the question as to whether a similar challenge involving binding corporate rules could be next. In May 2017, the Irish High Court, announced that it will seek a referral to the CJEU in respect of privacy campaigner Max Schrem’s complaint against Facebook in respect of model contracts. This opens up the possibility of a CJEU ruling unfavourable to the use of model contracts.

Finally, the adoption of the NIS Directive in 2016, which must be implemented into national laws by May 2018, means that the next few months are likely to see Member States consulting on or proposing implementing legislation. Given the increased risk of cyberattacks against organisations, it is hoped that these new provisions will strengthen the EU cyberbreach strategy and reduce the risk of organised cybercrime. Organisations should review the provisions of the NIS Directive and of any draft or finalised Member State implementing legislation and begin amending their cybersecurity practices and procedures to ensure compliance.
APEC OVERVIEW

Ellyce R Cooper and Alan Charles Raul

I OVERVIEW

The Asia-Pacific Economic Cooperation (APEC) is an organisation of economic entities in the Asia-Pacific region formed to enhance economic growth and prosperity in the region. It was established in 1989 by 12 Asia-Pacific economies as an informal ministerial-level dialogue group. Because APEC is primarily concerned with trade and economic issues, the criterion for membership is being an economic entity rather than a nation. For this reason, its members are usually described as ‘APEC member economies’ or ‘APEC economies’. Since 1993, the heads of the member economies have met annually at an APEC Economic Leaders Meeting, which has since grown to include 21 member economies as of September 2017: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the United States and Vietnam. Collectively, the 21 member economies account for more than half of world real GDP in purchasing power parity and over 44 per cent of total world trade.

The main aim of APEC is to fulfil the goals established in 1994 at the Economic Leaders Meeting in Bogor, Indonesia of free and open trade and investment in the Asia-Pacific area for both industrialised and developing economies. APEC established a framework of key areas of cooperation to facilitate achievement of these ‘Bogor Goals’. These areas, also known as the three pillars of APEC, are the liberalisation of trade and investment, business facilitation and economic and technical cooperation. In recognition of the exponential growth and transformative nature of electronic commerce, and its contribution to economic growth in the region, APEC established an Electronic Commerce Steering Group (ECSG) in 1999, which began to work towards the development of consistent legal, regulatory and policy...
environments in the Asia-Pacific area. Because of varied domestic privacy laws among the member economies (including economies at different stages of legislative recognition of privacy), APEC concluded that a regional agreement that creates a minimum privacy standard would be the optimal mechanism for facilitating the free flow of data among the member economies (and thus promoting electronic commerce). The result was the principles-based APEC Privacy Framework, which was endorsed by the APEC economies in 2004. Although consistent with the original Organisation for Economic Co-operation and Development (OECD) Guidelines, the APEC Privacy Framework also provided assistance to member economies in developing data privacy approaches that would optimise the balance between privacy protection and cross-border data flows.

Unlike other privacy frameworks, APEC does not impose treaty obligation requirements on its member economies. Instead, the cooperative process among APEC economies relies on non-binding commitments, open dialogue and consensus. Member economies undertake commitments on a voluntary basis. Consistent with this approach, the APEC Privacy Framework is advisory only and thus has few legal requirements or constraints.

APEC recently developed the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. In 2015, APEC developed the Privacy Recognition for Processors (PRP) system, a corollary to the CBPR system for data processors. APEC is also working with the EU to study the potential interoperability of the APEC and EU data privacy regimes, and in 2014 issued a joint referential document that maps the requirements of the two regimes for the benefit of businesses that seek certification or approval under both systems. A common questionnaire and a referential document for processors are also under development.

The APEC Privacy Framework, the CBPR and PRP systems, the cooperative privacy enforcement system and the ‘APEC–EU Referential’ are all described in more detail below.

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework was developed to promote a consistent approach to information privacy protection in the Asia-Pacific region as a means of ensuring the free flow of information in support of economic development. It was an outgrowth of the 1998 APEC Blueprint for Action on Electronic Commerce, which recognised that the APEC member economies needed to develop and implement legal and regulatory structures to build public

---

4 The ECSG was originally established as an APEC senior officials’ special task force, but in 2007 was realigned to the Committee on Trade and Investment. This realignment underscores the focus within the ECSG, and its Data Privacy Subgroup, on trade and investment issues.

5 APEC endorsed the Blueprint in 1998 to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy. See APEC Privacy Framework, Paragraph 1 (available at www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx).
confidence in the safety and security of electronic data flows (including consumers’ personal data) to realise the potential of electronic commerce. This recognition was the impetus behind the development of the Privacy Framework. Thus, the APEC objective of protecting informational privacy arises in the context of promoting trade and investment, rather than primarily to protect basic human rights as in the European Union.

The APEC Privacy Framework represents a consensus among economies with different legal systems, cultures and values, and that at the time of endorsement were at different stages of adoption of domestic privacy laws and regulations. Thus, the Framework provided a basis for the APEC member economies to acknowledge and implement basic principles of privacy protection, while still permitting variation among them. It further provides a common basis on which to address privacy issues in the context of economic growth and development, both among the member economies and between them and other trading entities.

ii The Privacy Framework

The Privacy Framework has four parts:

a Part I is a preamble that sets out the objectives of the principles-based Privacy Framework and discusses the basis on which consensus was reached;
b Part II describes the scope of the Privacy Framework and the extent of its coverage;
c Part III sets out the information privacy principles, including an explanatory commentary on them; and
d Part IV discusses the implementation of the Privacy Framework, including providing guidance to member economies on options for domestic implementation.

Objectives and scope of the Privacy Framework (Parts I and II)

The market-oriented approach to data protection is reflected in the objectives of the Privacy Framework, which include – in addition to the protection of information – the prevention of unnecessary barriers to information flows, the promotion of uniform approaches by multinational businesses to the collection and use of data, and the facilitation of domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework was designed for broad-based acceptance across member economies by encouraging compatibility while still respecting the different cultural, social and economic requirements within the economies. As such, it sets an advisory minimum standard and permits member economies to adopt stronger, country-specific data protection laws.

The Privacy Framework cautions that the principles should be interpreted as a whole, rather than individually, because they are interconnected, particularly in how they balance privacy rights and the market-oriented public interest. These principles are not intended to impede governmental activities within the member economies that are authorised by law, and thus the principles allow exceptions that will be consistent with particular domestic circumstances.6 The Framework specifically recognises that there ‘should be flexibility in implementing these Principles’.7

---

7 See APEC Privacy Framework, Paragraph 12.
The nine principles of the Privacy Framework (Part III)

Given that seven of the original APEC member economies were members of the OECD, it is not surprising that the APEC Privacy Framework was based on the original OECD Guidelines. The APEC privacy principles address personal information about living individuals and exclude both publicly available information and information connected with domestic affairs. The principles apply to persons or organisations in both public and private sectors who control the collection, holding, processing or use of personal information. Organisations that act as agents for others are excluded from compliance.

While based on the OECD Guidelines, the APEC principles are not identical to them. Missing are the OECD Guidelines of ‘purpose specification’ and ‘openness’, although aspects of these can be found within the nine principles – for example, purpose limitations are incorporated in Principle IV regarding use of information. The APEC principles also permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines on notice. In general, the APEC principles reflect the objective of promoting economic development and the respect for differing legal and social values among the member economies.

Principle I – preventing harm
This principle provides that privacy protections be designed to prevent harm to individuals from wrongful collection or misuse of their personal information and that remedies for infringement be proportionate to the likelihood and severity of harm.

Principle II – notice
The notice principle addresses the information that a data controller must include in a notice to individuals when collecting their personal information. It also requires that all reasonable steps be taken to provide the notice either before or at the time of collection and if not, then as soon after collection as is reasonably practicable. The principle further provides for an exception for notice of collection and use of publicly available information.

Principle III – collection limitation
This principle provides for the lawful and fair collection of personal information limited to that which is relevant to the purpose of collection and, where appropriate, with notice to, or consent of, the data subject.

Principle IV – uses of personal information
This principle limits the use of personal information to those uses that fulfil the purpose of collection and other compatible or related purposes. It includes exceptions for information collected with the consent of the data subject and collection necessary to complete a request of the data subject or as required by law.

Principle V – choice
The choice principle directs that, where appropriate, individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information, with an exception for publicly available information. This principle also contemplates that, in some instances, consent can be implied or is not necessary.
Principle VI – integrity of personal information
This principle states that personal information should be accurate, complete and kept up to date to the extent necessary for the purpose of use.

Principle VII – security safeguards
This principle requires that security safeguards be applied to personal data that are appropriate and proportional to the likelihood and severity of threatened harm, the sensitivity of the data and the context in which it is held, and that the safeguards be periodically reassessed.

Principle VIII – access and correction
The access and correction principle directs that individuals have the right of access to their personal information within a reasonable time and in a reasonable manner, and may challenge its accuracy and request appropriate correction. This principle includes exceptions when the burden of access or correction outweighs the risks to individual privacy, the information is subject to legal or security holds, or where privacy rights of other data subjects may be affected.

Principle IX – accountability
This principle requires that a data controller be accountable for complying with measures that give effect to the nine principles and that, when transferring personal information, it should take reasonable steps to ensure that the recipients also protect the information in a manner that is consistent with the principles. This has often been described as the most important innovation in the APEC Privacy Framework and it has been influential in encouraging other privacy regulators to consider similar accountability processes tailored to the risks associated with that specific data.

Unlike other international frameworks, the APEC Privacy Framework neither restricts the transfer of data to countries without APEC-compliant data protection laws nor requires such a transfer to countries with APEC-compliant laws. Instead, APEC adopted the accountability principle in lieu of data import and export limitations as being more consistent with modern business practices and the stated objectives of the Privacy Framework.

Implementation (Part IV)
Because APEC is a cooperative organisation, the member economies are not required to convert the Privacy Framework into domestic legislation. Rather, the Privacy Framework encourages the member economies to implement it without requiring or proposing any particular means of doing so. It suggests that there are 'several options for giving effect to the Framework [. . .] including legislative, administrative, industry self-regulatory or a combination of these methods'. The Framework advocates 'an appropriate array of remedies [. . .] commensurate with the extent of the actual or potential harm' and supports a choice of remedies appropriate to each member economy. The Privacy Framework does not contemplate a central enforcement entity.

Thus, the APEC Privacy Framework contemplates variances in implementation across member economies. It encourages member economies to share information, surveys and
research and to engage in cross-border cooperation in investigation and enforcement.\textsuperscript{10} This concept later developed into the Cross-Border Privacy Enforcement Arrangement (CPEA – see Section III.iii).

iii  Data privacy individual action plans (IAPs)

Data privacy IAPs are periodic, national reports to APEC on each member economy’s progress in adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.\textsuperscript{11} The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2017, 14 member economies have posted IAPs on the APEC website.\textsuperscript{12}

III  APEC CROSS-BORDER DATA TRANSFER

i  Data Privacy Pathfinder initiative

The APEC Privacy Framework does not explicitly address the issue of cross-border data transfer, but rather calls for cooperative development of cross-border privacy rules.\textsuperscript{13} In 2007, the APEC ministers endorsed the APEC Data Privacy Pathfinder initiative with the goal of achieving accountable cross-border flows of personal information within the Asia-Pacific region. The Data Privacy Pathfinder initiative contains general commitments leading to the development of an APEC CBPR system that would support accountable cross-border data flows consistent with the APEC Privacy Principles.

The main objectives of the Pathfinder initiative are to promote a conceptual framework of principles for the execution of cross-border privacy rules across APEC economies, to develop consultative processes among the stakeholders in APEC member economies for the development of implementing procedures and documents supporting cross-border privacy rules and to implement an accountable cross-border privacy system. Since 2008, the Data Privacy Subgroup has been working on nine interrelated projects to support the development of cross-border privacy rules in the Asia-Pacific region. Both the CBPR system and the CPEA are outcomes of the Pathfinder initiative.

ii  The CBPR system

The APEC CBPR system, endorsed in 2011, is a voluntary accountability-based system governing electronic flows of private data among APEC economies. As a newly established system, the CBPR system is in the early stages of implementation. As of September 2017, five APEC economies participate in the CBPR system – Canada, Japan, Mexico, South Korea and the United States – with more expected to join.

In general, the CBPR system requires businesses to develop their own internal privacy-based rules governing the transfer of personal data across borders under standards that meet or exceed the APEC Privacy Framework. The system is designed to build consumer, business and regulator trust in the cross-border flow of electronic personal data in the

\begin{footnotesize}
\begin{enumerate}
\item See APEC Privacy Framework, Paragraphs 40–45.
\item See APEC Privacy Framework, Paragraph 39.
\item See www.apec.org/Groups/Committee-on-Trade-and-Investment/-/link.aspx?id=CB717EE6184848D396f31D8B814E5C90&z=z.
\item See APEC Privacy Framework, Paragraphs 46–48.
\end{enumerate}
\end{footnotesize}
Asia-Pacific region. One of the goals of the CBPR system is to ‘lift the overall standard of privacy protection throughout the [Asia-Pacific] region’ through voluntary, enforceable standards set out within it.14

Organisations that choose to participate in the CBPR system must submit their privacy practices and policies for evaluation by an APEC-recognised accountability agent to assess compliance with the programme. Upon certification, the practices and policies will become binding on that organisation and enforceable through the relevant privacy enforcement authority.15

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, which is composed of nominated representatives of participating economies and any working groups the Panel establishes. The Joint Oversight Panel operates according to the Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.16

Accountability agents and privacy enforcement authorities are responsible for enforcing the CBPR programme requirements, either under contract (private accountability agents) or under applicable domestic laws and regulations (accountability agents and privacy enforcement authorities).

The CBPR system has its own website, which includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports and template forms.17

**Participation in the CBPR system**

Only APEC member economies may participate in the CBPR system and must meet three requirements:

\[a\] participation in the APEC CPEA with at least one privacy enforcement authority;

\[b\] submission of a letter of intent to participate addressed to the chairs of the APEC ECSG, the Data Privacy Subgroup and the CBPR system Joint Oversight Panel providing:

- confirmation of CPEA participation;
- identification of the APEC CBPR system-recognised accountability agent that the economy intends to use; and
- details regarding relevant domestic laws and regulations, enforcement entities and enforcement procedures; and

\[c\] submission of the APEC CBPR system programme requirements enforcement map.

15 A privacy enforcement authority is ‘any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings’. ‘Privacy Law’ is further defined as ‘laws and regulations of an APEC Economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework’. APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, at 10.
16 See cbprs.blob.core.windows.net/files/JOP%20Charter.pdf; and cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf.
17 See www.cbprs.org/default.aspx.
The Joint Oversight Panel of the CBPR issues a findings report that addresses whether the economy has met the requirements for becoming an APEC CBPR system participant. An applicant economy becomes a participant upon the date of a positive findings report.

**Accountability agents**

The APEC CBPR system uses APEC-recognised accountability agents to review and certify participating organisations’ privacy policies and practices as compliant with the APEC CBPR system requirements, including the APEC Privacy Framework. Applicant organisations may participate in the CBPR system only upon this certification and it is the responsibility of the relevant accountability agent to undertake certification of an applicant organisation’s compliance with the programme requirements. An accountability agent makes no determination as part of the CBPR verification programme regarding whether the applicant organisation complies with domestic legal obligations that may differ from the CBPR system requirements.

APEC CBPR system requirements for accountability agents include:

- **a** being subject to the jurisdiction of a privacy enforcement authority in an APEC economy participating in the CBPR system;
- **b** satisfying the accountability agent recognition criteria;\(^{18}\)
- **c** agreeing to use the CBPR intake questionnaire to evaluate applicant organisations (or otherwise demonstrate that propriety procedures meet the baseline requirements of the CBPR system); and
- **d** completing and signing the signature and contact information form.\(^{19}\)

Proposed accountability agents are nominated by an APEC member economy and, following an application and review process by the Joint Oversight Panel, may be approved by the ECSG upon recommendation by the Panel. Any APEC member economy may review the recommendation as to any proposed accountability agent and present objections to the ECSG. Once an application has been approved by the ECSG, the accountability agent is deemed ‘recognised’. Complaints about a recognised accountability agent are reviewed by the Joint Oversight Panel, which has the discretion to request investigative or enforcement assistance from the relevant privacy enforcement authority in the APEC economy where the agent is located.

No accountability agent may have an actual or potential conflict of interest, nor may it provide services to entities it has certified or that have applied for certification. It must continue to monitor certified organisations for compliance with the APEC CBPR system standards and must obtain annual attestations regarding this compliance. It must publish its certification standards and must promptly report all newly certified entities, as well as any suspended or terminated entities to the relevant privacy enforcement authorities and the CBPR Secretariat.

Accountability agents can be either public or private entities and may also be a privacy enforcement authority. Under certain circumstances, an APEC economy may designate an accountability agent from another economy.

Accountability agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities.

\(^{18}\) See cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf.  
\(^{19}\) See cbprs.blob.core.windows.net/files/Signature%20and%20Contact%20Information.pdf.
If only one accountability agent operates in an APEC economy and it ceases to function as an accountability agent for any reason, then the economy’s participation in the CBPR system will be suspended and all certifications issued by that accountability agent for businesses will be terminated until the economy once again fulfils the requirements for participation and the organisations complete another certification process.

The CBPR system website contains a chart of recognised accountability agents, their contact information, date of recognition, approved APEC economies for certification purposes and links to relevant documents and programme requirements.\(^{20}\)

As of September 2017, the CBPR system recognises two accountability agents: TRUSTe and the Japan Institute for Promotion of Digital Economy and Community. TRUSTe is recognised to certify only organisations subject to the jurisdiction of the United States Federal Trade Commission (FTC). The Japan Institute for Promotion of Digital Economy and Community (now called JIPDEC) is recognised to certify organisations under the jurisdiction of the Ministry of Economy, Trade and Industry Government of Japan.

**CBPR system compliance certification for organisations**

Only organisations that are subject to the laws of one or more APEC CBPR system-participating economies are eligible for certification regarding personal information transfers between economies.

An organisation that chooses to participate in the CBPR system initiates the process through submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised accountability agent. The accountability agent will then undertake an iterative evaluation process to determine whether the organisation meets the baseline standards of the programme. The accountability agent has sole responsibility for these first two phases of the CBPR system accreditation process (self-assessment and compliance review).

Organisations that are found to be in compliance with the programme requirements will be certified as CBPR-compliant and identified on the CBPR website. As of January 2017, more than 15 organisations have been APEC CBPR certified, all of which are in the United States, with more in various stages of review.\(^{21}\) Certified companies must undergo annual recertification. As more accountability agents are recognised in the economies participating in the CBPR system, the number of certified organisations is expected to grow.

**Effect of the CBPR on domestic laws and regulations**

The CBPR system sets a minimum standard for privacy protection requirements and thus an APEC economy may need to make changes to its domestic laws, regulations and procedures to participate in the programme. With that exception, however, the CBPR system does not otherwise replace or modify any APEC economy’s domestic laws and regulations. Indeed, if the APEC economy’s domestic legal obligations exceed those of the CBPR system, then those laws will continue to apply to their full extent.

\(^{20}\) See www.cbprs.org/Agents/AgentDetails.aspx.

\(^{21}\) A current list of APEC-certified organisations can be found at cbprs.blob.core.windows.net/files/APEC%20CBPR%20Compliance%20Directory_Jan2017%20APECCBPRComplianceDirectory.pdf.
PRP system

Because the CBPR system (and the APEC Framework) applies only to data controllers, who remain responsible for the activities conducted by processors on their behalf, APEC member economies and data controllers encouraged the development of a mechanism to help identify qualified and accountable data processors. This led, in 2015, to the APEC PRP programme, which is a mechanism by which data processors can be certified by an accountability agent. 

This certification can provide assurances to APEC economies and data controllers regarding the quality and compatibility of the processor’s privacy policies and practices. The PRP does not change the allocation of responsibility for the processor’s practices to the data controller and there is no requirement that a controller engage a PRP-recognised processor to comply with the Framework’s accountability principle.

APEC is in the process of integrating the PRP system into the CBPR governance system and it is expected that the PRP system will follow the same model. Differences in national laws among APEC economies, however, necessarily result in different enforceability options under the PRP system and how each economy will support enforcement is not yet finalised.

iii The CPEA

One of the key goals of the Privacy Framework is to facilitate domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework does not establish any central enforcement body, but instead encourages the cooperation of privacy enforcement authorities within the Asia-Pacific region. APEC established the CPEA as a multilateral arrangement to facilitate such interaction. The CPEA became the first mechanism in the Asia-Pacific region to promote cooperative assistance among privacy enforcement authorities.

Among other things, the CPEA promotes voluntary information sharing and enforcement by:

a. facilitating information sharing among privacy enforcement authorities within APEC member economies;

b. supporting effective cross-border cooperation between privacy enforcement authorities through enforcement matter referrals and parallel or joint enforcement actions; and

c. encouraging cooperation and information sharing with enforcement authorities of non-APEC member economies.

The CPEA was endorsed by the APEC ministers in 2009 and commenced in 2010 with five participating economies: Australia, China, Hong Kong China, New Zealand and the United States. Any privacy enforcement authority from any APEC member economy may participate and each economy may have more than one participating privacy enforcement authority. As of September 2017, CPEA participants included over two dozen Privacy Enforcement Authorities from 10 APEC economies.

---

22 The PRP Purpose and Background Document can be found at cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf; and the intake questionnaire for processors is at cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf.

Under the CPEA, any privacy enforcement authority may seek assistance from a privacy enforcement authority in another APEC economy by making a request for assistance. The receiving privacy enforcement authority has the discretion to decide whether to provide such assistance.

Participation in the CPEA is a prerequisite to participation by an APEC economy in the CBPR system. As a result, each participating APEC economy must identify an appropriate regulatory authority to serve as the privacy enforcement authority in the CBPR system. That privacy enforcement authority must be ready to review and investigate a CBPR complaint if it cannot be resolved by the certified organisation or the relevant accountability agent, and take whatever enforcement action is necessary and appropriate. As more member economies join the CBPR system, this enforcement responsibility is likely to become more prominent.

IV  INTEROPERABILITY

Given the global nature of personal information flows, APEC’s Data Privacy Subgroup has been involved in collaborative efforts with other international organisations with the goal of improving trust and confidence in the protection of personal information and, ultimately, to enable the associated benefits of electronic commerce to flourish across the APEC region. While privacy regimes such as the APEC Privacy Framework are drafted at the level of principles, there are often very significant differences in the legal and policy implementation of those principles in different economies around the world. In an effort to bridge those differences and find commonality between the two largest privacy systems – the APEC Privacy Framework and the EU Data Protection Directive – in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes.

In early 2014, the APEC/EU Working Group released a reference document (endorsed by APEC Senior Leaders in February 2014) that maps the CBPR system requirements and the binding corporate rules (BCRs) under the EU Data Protection Directive and identifies commonalities and differences between the two (the Referential).\(^\text{24}\) This document provides an important tool to multinational companies in developing global privacy compliance procedures that are compliant with both systems. Because it is set up in a block format, laying out the areas of commonality and the additional requirements of each privacy regime, the Referential provides a comparative tool that can be used as a checklist by companies seeking or considering certification by one or both systems. It does not, however, create interoperability or mutual recognition of the regimes.

The Referential points out that such companies still need to be approved by each of the relevant bodies in both EU Member States and APEC economies. The Referential further cautions against using the document itself as an organisation’s proposed framework, because each organisation’s privacy policies should be tailored to that organisation. Moreover, data processed in an APEC economy is still subject to that economy’s domestic laws. And whenever the APEC CBPR system is incompatible with the EU Data Protection Directive, the organisation must affirmatively describe the circumstances under which it will apply the rules of one system rather than the other.

Following the Referential, the Article 29 Working Party and the APEC Data Privacy Subgroup agreed to develop additional practical tools to help organisations to become certified under both the BCR and CBPR systems. The joint working group has committed

\(^{24}\) See www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.
to developing a common application form based on each system’s intake questionnaires that can be submitted, along with a mapping of the company policies and associated personal data and privacy programme practices and effectiveness tools, to support certification in both systems. The joint working group will also work, over the long term, to develop a common Referential for mapping requirements for processors under the BCR and CBPR systems.

The Referential and the common application are important steps towards developing policies, practices and enforcement procedures that could apply to both systems and perhaps – eventually – a common framework.

V THE YEAR IN REVIEW AND OUTLOOK

The Data Privacy Subgroup is undertaking a 10-year review and evaluation (stocktake) of domestic and international implementation of the APEC Privacy Framework through a working group established for that purpose and led by Australia. The member economies have been encouraged to update their IAPs in support of that stocktake. The stocktake will consider whether the APEC Privacy Framework should be updated to ensure relevance as the market evolves with technology innovations, such as big data, cloud computing and the internet of things. It will consider updating the Framework by addressing such topics as interoperability with other privacy frameworks, breach notifications, privacy management programmes and factors to consider when balancing economic and privacy interests.

On 12 June 2017, the South Korean government officially joined the United States (2012), Mexico (2013), Japan (2014) and Canada (2015) as an approved APEC economy participating in the APEC CBPR system.25 This system is growing slowly, as some economies are waiting to see interest from business and some businesses are waiting for member economies to join. With all the North American Free Trade Agreement countries participating, the CBPR system has taken an important step towards an international presence, which may encourage more APEC member economies and business organisations to participate. IBM became the first company to be certified under the APEC CBPR system, in August 2013; it has been joined by nearly two dozen others, including companies with significant international presence, such as Apple, HP and Merck. All these companies were certified by TRUSTe, the sole accountability agent at the time.

TRUSTe became the first recognised accountability agent under the CBPR system on 25 June 2013 and that status was renewed unanimously by the 21 APEC member economies in early 2015. In early 2016, the 21 APEC member economies approved JIPDEC as Japan’s accountability agent. Mexico and Canada have not yet identified their domestic accountability agents.

On 12 July 2016, the EU adopted the EU–US Privacy Shield. The purpose of the Privacy Shield is to provide rights to EU citizens whose personal data is transferred to the United States and clarify the requirements for businesses performing transatlantic data transfers. US companies transferring data into the European market should look to both the EU–US Privacy Shield and APEC’S CBPR for guidance.

Following its first enforcement decision under the CBPR against Very Incognito Technologies Inc in June 2016 for misrepresenting its compliance with the CBPR,26 the FTC continues to bring enforcement actions under APEC. Over the past year, the FTC

reached settlements with three additional companies – Sentinel Labs, Inc, SpyChatter, Inc and Vir2us, Inc, – in actions where the FTC alleged the companies had misrepresented consumers about their participation in the APEC CBPR system.27 According to the FTC’s allegations, all three companies’ privacy policies misrepresented that the companies either ‘comply with the APEC CBPR’ or ‘abide by the APEC CBPR’. To settle, the companies signed consent agreements that prohibit them from making misrepresentations about their participation, membership or certification in any privacy or security programme sponsored by a government or self-regulatory or standard-setting organisation.

These cases followed the FTC’s announcement in 2016 that it had sent warning letters to 28 companies who claimed compliance with the CBPR despite failing to meet the CBPR requirements. The combination of the first enforcement action and the large number of enforcement letters indicates that the FTC has brought actions against other companies for similar misrepresentations in other transborder programmes, such as the US–EU Safe Harbor Framework and recently under the Privacy Shield as well. The FTC has reminded companies not to mislead consumers about participation in the new EU–US Privacy Shield programme. These new enforcement decisions and warnings indicate that the FTC may play a more active role in the future enforcement of the CBPR.

I OVERVIEW

Data protection was introduced to the Argentine legal system following the 1994 constitutional reform, with the incorporation of the habeas data procedure. With this constitutional reform, data protection rights in Argentina acquired constitutional protection and, thus, are considered fundamental rights that cannot be suppressed or restricted without sufficient cause.

In October 2000, Congress passed Law No. 25,326 (the Data Protection Law), which focused directly on data protection. It defined several data protection-related terms and included general principles regarding data collection and storage, outlining the data owner’s rights and setting out the guidelines for the treatment of personal data. It is an omnibus law largely based on the EU Data Protection Directive and the subsequent local legislation issued by the European countries (mainly Spain). Moreover, on 30 June 2003, the European Union issued a resolution establishing that Argentina had a level of protection consistent with the protection granted by the Directive with respect to personal data.

Additionally, the Data Protection Law created the enforcement authority embodied by the National Data Protection Agency (the Data Protection Agency), which is the office in charge of enforcing the data protection regulations, controlling the registration of databases, assisting individuals regarding their rights, receiving claims and carrying out inspections of companies to assess their compliance with the Data Protection Law.

In 2014, Law No. 26,951 (the Do-Not-Call Law) created the do-not-call registry and expanded the protection of data owner’s rights. This regulation is enforced by the Data Protection Agency and allows the 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 Data Protection Agency and consult the list of blocked numbers on a monthly basis before engaging in marketing calls.
II THE YEAR IN REVIEW

During the early months of 2017, Justice 2020, a governmental initiative for the design of public policies promoted by the Ministry of Justice together with the Data Protection Agency, proposed amendments to the Data Protection Law and the Do Not Call Law. As of 15 September 2017, this draft bill (the Draft) has yet to be submitted to the legislative branch of government.

The Draft defines new data protection-related terms and clarifies other terms defined by the Data Protection Law.

One of its most relevant changes is the scope of application and jurisdiction of the law, which is not currently regulated by the Data Protection Law. If it is passed, this new law will apply in the following cases: (1) when the person responsible for the treatment is domiciled in Argentina, even if the data treatment takes place abroad; (2) when the person responsible for the data treatment is not based in Argentina but in a place where Argentine legislation applies by virtue of international law; and (3) when the data treatment of data owners that reside in Argentina is performed by an entity with responsibility for data treatment that is not based in Argentina but whose data-treatment activities are related to the offer of goods or services to data owners in Argentina, or to the monitoring of their acts, behaviour or interests.4

With this new wording, the Draft specifically recognises that data treatment involving Argentine residents’ personal data can occur abroad and grants the same protections as if the treatment had taken place in Argentina.

The Draft also includes new valid ways for obtaining the data owners’ consent for the treatment of their personal data,5 stating that express consent may be granted in writing, orally or through electronic means or any other similar means that technology may offer.

Moreover, the concept of tacit consent6 is introduced. Tacit consent shall be deemed granted by the data owner when (1) it emerges clearly from the context of the data treatment; (2) the conduct of the data owner is sufficient to demonstrate the existence of the relevant authorisation; (3) the data requested is necessary for the purpose of the collection; and (4) the data owner has been informed of his or her rights arising from the law.

The Draft, following the principles set out in the Data Protection Law, expressly prohibits the treatment of sensitive data, with the following exceptions: (1) the data owner has granted his or her express consent to the treatment; (2) the treatment is necessary for the fulfilment of labour and social security obligations in relation to the data treatment itself or to the data owner; (3) the treatment is necessary for the recognition, exercise or defence of rights in a judicial procedure; or (4) the treatment has a historical, statistical or scientific purpose, in which case dissociation of data must take place.

Following the recent Regulation (EU) 2016/679 of the European Parliament and of the Council, the Draft expressly addresses and regulates the consent given by children or teenagers for the treatment of their personal data.7 The Draft establishes that such consent shall be deemed valid when it is applied to the processing of data directly linked to information services specifically designed and suitable for children or teenagers. Teenagers can grant

---

4 Section 4 of the Draft.
5 Section 12 of the Draft.
6 Section 12 of the Draft.
7 Section 18 of the Draft.
their consent from 13 years of age. For children less than 13 years old, the treatment of their personal data shall be considered lawful only if consent is granted by the child’s parent or guardian.

Another relevant addition by the Draft is the inclusion of a procedure to be carried out by data processors in the event of data breaches. The Draft incorporates the obligation for the person responsible for the data treatment to document and report data incidents to the data owner and the enforcement authority with no delay, and preferably within 72 hours of the acknowledgment of the security breach, unless the breach is unlikely to present a risk to the data owner.8

With this key modification, the Draft regulates standard procedures, providing guidelines for dealing with security breaches, which the Data Protection Law does not address. Regarding the data owner’s rights,9 the Draft extends the scope of the information to be provided to the data owner when exercising its right of access, stating that the data owner must be informed of not only the existing data, but also, inter alia, (1) the recipients or categories of recipients to whom the personal data has been or will be transferred; and (2) the existence of automatic decision-making processes, including profiling.

Additionally, the right to data portability is incorporated,10 which establishes that when electronic services that comprise personal data treatment are provided, the data owner will have the right to obtain from the person responsible a copy of the personal data in a structured and commonly used format that allows its subsequent use or its direct transference from responsible entity to responsible entity when it is technically possible.

With respect to users and managers of files, records and databases, specific guidelines related to proactive responsibility are established:11 among the technical and organisational measures to be taken, the person responsible for the treatment should include inter alia, internal or external audits, the adoption of a ‘privacy policy’ or the adherence to binding self-regulatory mechanisms to be submitted for approval by the enforcement authority. In particular, it is ordered that measures should be taken to ensure that, by default, only personal data necessary for each of the purposes of the data treatment are processed.

Another relevant addition is the requirement for the creation of a data protection officer,12 who must be appointed when sensitive data or large-scale data treatment is carried out. The data protection officer’s responsibilities include, inter alia, internal advice and compliance duties in connection to data protection issues.

Binding self-regulating mechanisms are encouraged, and should be filed with the enforcement authority for approval.

The Draft also excludes the possibility of legal entities registering with the do-not-call registry to block contact.13

8 Section 20 of the Draft.
9 Section 28 of the Draft.
10 Section 33 of the Draft.
11 Section 37 of the Draft.
12 Section 43 of the Draft.
13 Section 49 of the Draft.
III  REGULATORY FRAMEWORK

i  Privacy and data protection legislation and standards

As expressed above, the Data Protection Law is an omnibus law that regulates data protection in a comprehensive manner. In contrast to other jurisdictions (particularly the United States), Argentina does not have other specific data protection regulations outside the scope of the Data Protection Law, and there is no related legislation at a subnational level.

The Data Protection Law includes principles regarding data protection, data owners’ rights, the organisation of data archives and databases, and actions to protect personal data, to mention a few.

The Law’s main purposes are (1) to protect personal data stored in archives, registers, databanks or other technical means of data processing; (2) to guarantee people’s honour and privacy; and (3) to ensure data owners their rights to access records of their data stored and treated by third parties.

As is the case with most omnibus data protection laws around the world, the Data Protection Law contains several defined terms that are essential for interpreting the Law and determining its scope of application. Some of the main defined terms are:

a  personal data: information of any kind referring to an individual or legal person, either determined or determinable;

b  sensitive data: personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral convictions, union affiliation and information concerning health or sexual life;

c  person responsible for the registry or database: the individual or legal entity that is the owner of a file, registry or database; and

d  data owner: any individual or legal entity residing in Argentina whose data is the object of the treatment referred to in this Law.

The following are the main principles expressed by the Data Protection Law:

a  due registration: data storage will be lawful if the database is duly registered with the Data Protection Agency; and

b  data quality: 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. The collection of personal data cannot be done by unfair or fraudulent means. Personal data subject to treatment cannot be used for purposes different from or incompatible with those leading to their collection.

The main rights for data owners contained in the Data Protection Law are the right of information, access and suppression: exercising this information right, data owners can request from the person responsible for the database their personal information that has been collected, the purpose of the collection and the identity of the person responsible for it. Additionally, personal data that is totally or partially inaccurate or incomplete should be deleted and replaced or, if necessary, completed by the file manager when the inaccuracy or incompleteness of the information is known. Data owners do not have to pay to exercise these rights. This right of access can be exercised (1) directly, through the person responsible for the database; (2) through the Data Protection Agency; or (3) through the habeas data procedure. To guarantee these rights, data must be stored in a way that allows the exercise of the right of access of the owner. Data must be destroyed when it is no longer necessary or relevant for the purposes for which it was collected.
ii General obligations for data handlers

The first obligation for data handlers is to obtain consent from data owners. The treatment of personal data is unlawful when the data subject has not given his or her express consent to the treatment of the data, either in writing or through any other similar means. The consent must appear in a clear and unequivocal manner. There are certain exceptional cases in which consent is not requested, such as when the personal data (1) derives from unrestricted public-access sources; (2) is collected for the performance of public duties; (3) is limited to name, identification card number, tax or social security identification, occupation, date of birth, domicile and telephone number; (4) arises from a contractual relationship and is necessary for the fulfilment of that contract; or (5) refers to the transactions performed by financial entities and arises from the information provided by their customers.

Another important obligation for database owners is the obligation for registration with the Data Protection Agency. To file the registration, the company or individual responsible for the database must provide information regarding the location of the database, its characteristics and purpose, specifications of the data provided, origin, means of collection, etc. This registration must be renewed annually. The registration process is simple and relatively inexpensive.

iii Specific regulatory areas

The Data Protection Law contains several specific regulations applicable to different areas and industries.

One of the most relevant areas is financial information provided by private registries issuing reports. In that sense, to analyse a prospective client's financial records it is common for banks and other financial entities to seek credit information through different credit information services.

The Data Protection Law specifies which information can be treated. First, it needs to be personal data of an economic nature and it must be obtained from public sources or have been given by the data owner or collected with the data owner's consent.

Additionally, information regarding the fulfilment (or not) of a party's financial obligations can be given by the creditor (or by someone acting on its behalf), since both parties are owners of the information. In this case, there is no need to obtain the other party's consent.

Information relevant for the assessment of someone's financial capacity can be stored, registered or transferred for a maximum of five years. If the debtor cancels the debt, or it expires by any means, the period shall be reduced to two years. This issue tends to generate a substantial number of claims from consumers and users of financial services.

The Data Protection Law regulates the treatment of personal data by health institutions too. Public and private hospitals and health professionals can process their patients’ data relating to mental or physical health, as long as they respect professional secrecy.

These registries are very useful for scientific purposes, but it is important to note that they store sensitive data and dissociation of data is advised.

Furthermore, security and surveillance industries are also regulated and are currently the focus of most of the inspections carried out by the Data Protection Agency. Disposition 10/2015 regulates the use of closed-circuit television cameras in public spaces. The Disposition establishes that the use of these cameras is lawful when the data handler has obtained the data owner's prior and informed consent. Consent shall be deemed as granted by the data owner if the data collector includes signs indicating the existence of these cameras,
the purpose of the data collection, the person responsible for the treatment and the relevant contact information. A template of this sign is included in the Disposition. The relevant database must be registered and the data collector must implement a manual for its use.

iv Technological innovation

The Data Protection Law has not been amended recently. For that reason, several technological innovations fall outside its scope.

The use of cookies, for example, was not included in the legislation. Nevertheless, by application of the Data Protection principles, companies trying to obtain information through them must obtain the user's consent to collect information.14

The use of big data, on the other hand, presents a much deeper issue. Through big data, companies collect big amounts of information and its different uses are not always clearly determinable since data is often reused – so violating one of the Data Protection Law's main principles, which is specifying to the data owner the purpose of the data collection. Moreover, data treated must be accurate, true and not excessive in relation to the purpose. In many cases, it is not possible to assess that all information is accurate. Because of the large volume of information provided, some of it is bound to be inaccurate.15 The Data Protection Law has fallen behind in regulating the use of big data. The collection of excessive amounts of information is only of benefit to the user, and regulation of big data must recognise this new and useful way of treating data and always respect the user's rights.

The Data Protection Agency has enacted several regulations aimed at reducing the technological gap generated between the enactment of the Data Protection Law and the present day. Besides the aforementioned Disposition 10/2015 on closed-circuit television cameras, a specific disposition regulating the use of drones has been enacted, setting out data privacy principles that apply to the use of these devices. Moreover, a recent disposition was enacted that contains best practice guidelines for data collection through apps.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Every nation that has specifically regulated data protection has realised that any form of planning and controlling would become useless if collected data could be automatically and unrestrictedly transferred abroad to be processed. Following the European model,16 the Data Protection Law has prohibited international data transfer when the transfer is to countries or international or supranational organisations that do not offer 'adequate levels of protection'.17

With this provision, Argentina has tried to avoid data being collected and treated in its territory without regulatory controls in place or without the data owner being able to exercise its rights. Where there are no regulatory controls in place or data owners are unable to exercise their rights, international data transfers are prohibited.

It will be considered that a country or organism has an adequate level of protection when those protections derive directly from the legal order, self-regulatory measures or contractual clauses that include specific data protection provisions.

---

14 Osvaldo Alfredo Gozaini, Habeas Data, Protection of Personal Data (Rubinzal-Culzoni), p. 325.
15 Luciano Gandola, 'Conflicts between Big Data and the Data Protection Law', Infojus.
16 See footnote 3.
17 Section 12 of the Data Protection Law.
Pursuant to Regulatory Decree 1558/2001, the Data Protection Agency is responsible for assessing the levels of protection granted by each country or organism, either ex officio or through consultation with a concerned party. If it considers that any given country or organisation does not provide adequate levels of protection, the Data Protection Agency must request the executive branch of the government to issue a declaration.

The offered levels of protection will be assessed in light of the data transfer's circumstances, the nature of the personal data involved, the duration of the treatment and the applicable law in the destination country, among other things.

Therefore, if the recipient party belongs to a country or organisation that does not comply with the Argentine legal requirements, it should adopt self-binding regulatory measures or contractual provisions covering protection for data owners.

In practice, the transferring party must assess the recipient's levels of protection and, if the recipient fails to offer protection at an adequate level legal, the transferring party must overcome this by obtaining the data owner's consent, or establishing contractual provision for an adequate level of protection.

Regulatory Decree 1558/2001 states that if the data owner has given its consent, it does not matter whether the state or organisation does not offer an adequate level of protection and, in that case, the international transfer can take place.

Additionally, consent is not necessary if the personal data is stored in a public registry legally created to provide information and that is open for public consultation or by anyone evidencing a legitimate interest.

The aforementioned prohibition will not apply in cases of (1) international judicial cooperation; (2) transfer of medical information, when the treatment of the deceased requires it, or in the case of an epidemic investigation; (3) bank or stock transfers; (4) transfers decided under international treaties to which Argentina is a party; and (5) when it takes place because of cooperation between agencies fighting organised crime, terrorism or drug trafficking.

V COMPANY POLICIES AND PRACTICES

Although it is not expressly set out in the legislation, companies are encouraged to implement a privacy policy that regulates their personal data collection, treatment and processing and security mechanisms. It is common for the Data Protection Agency to request this policy from companies upon inspections.

Additionally, Disposition 11/2006 of the Data Protection Agency requires companies to draft a security manual or report establishing the procedures and safety measures taken regarding personal data. The manual must describe the obligations of the employees regarding data treatment, the control measures implemented by the company, the applicable procedure upon information breaches or data-loss incidents, the measures for preventing malicious software, etc.

Disposition 10/2015 establishes that companies using closed-circuit television cameras must implement a policy that includes the means of data collection, a reference to the place, dates and hours of operation of the cameras, technical and confidentiality mechanisms to be used, ways of exercising the data owner's rights and, if applicable, reasons that justify obtaining a picture of the individuals entering the facilities.

18 Section 12 of Regulatory Decree 1558/2001.
Lastly, Disposition 18/2015 of the Data Protection Agency establishes ‘best practice guidelines for data collection through apps’. In addition to explaining specifically how data protection principles operate in this matter, the Disposition establishes that the privacy policy should be clear and easily accessible for users. Moreover, 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. The use of icons, pictures, distinctive colours and sounds is recommended; extra care is requested when the app is suitable for children or teenagers.

VI DISCOVERY AND DISCLOSURE

As stated above, data owners have several rights that derive from the Data Protection Law. Nevertheless, the rights of access, rectification and suppression can be denied when they could affect Argentina’s national security, order or public safety, or the protection of rights or interests of third parties.

Additionally, information regarding personal data can be denied when the disclosure of information could become an obstacle to judicial or administrative proceedings regarding tax matters, pension obligations, the development of health and environmental control functions, the investigation of criminal offences or the verification of administrative infringements. The resolution denying access must be reasoned and notified to the affected party, and must relate to the reasons established above.

Since these provisions include a limitation of rights, they should be interpreted restrictively. Additionally, to safeguard the data owner’s rights, this limitation must be subject to judicial review.

Despite all these provisions, the data owner must be able to access the registries if his or her defence rights rely on this action, in which case the access restriction must be lifted.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Data Protection Agency is the enforcement authority created by the Data Protection Law. Its lack of autonomy (it operates within the scope of the Ministry of Justice) has been subject to debate, and current plans involve the creation of a new autonomous entity in line with the criteria used in countries with the highest degree of personal data protection.

The agency’s main functions are (1) operating as a registry of databases, keeping records of the registration and renewal of databases; (2) enforcing the Data Protection Law and the Do-Not-Call Law, carrying out inspections and imposing sanctions; and (3) creating new dispositions and regulations related to data protection matters.

In using these powers, the Data Protection Agency has issued several dispositions relating to its investigatory and auditing powers. In this context, Disposition 55/2016 regulates the Data Protection Agency’s auditing procedures. The main aims of these proceedings are to control the activity of the person responsible for the database and ensure its compliance with the law.

The proceedings can be (1) ex officio, either scheduled annually or spontaneous; or (2) initiated upon a complaint, in which case the inspection itself will have an evidentiary nature.
After the inspection is finalised, the inspector will issue a final report with the outcome of the inspection. If the database owner has complied with the law, the proceeding is finalised. If it has not complied with the regulations, it is granted 15 days to remedy its non-fulfilment, otherwise sanctioning proceedings will begin.

ii Recent enforcement cases

The enforcement actions of the Data Protection Agency have evolved and intensified over the years. During its first years, the Agency’s role was more educational than punitive, giving companies ample time to adapt to the new legislation and being proactive in responding to enquiries and explaining misconceptions. Nowadays, 17 years after the enactment of the Data Protection Law, the Agency is being more proactive in carrying out inspections and is stricter with its enforcement and punitive capabilities.

The vast majority of recent fines have been for violation of the Do-Not-Call Law, resulting in a large number of administrative proceedings and claims. Some fines have also been imposed in the recent past on companies failing to comply with their obligations under the Data Protection Law (mainly failure to register or renew registrations for their databases and failure to comply with security measures).

On a judicial level, most of the case law regarding personal data protection is connected to financial companies and the information they provide to consumer credit reporting agencies regarding their customers’ debts. In most cases, the proceedings relate to financial companies’ failure to update their registries once debts have been paid or the statute of limitations applied.

In this context, the Supreme Court has also stated that the ‘right to be forgotten’ has constitutional rank and must be respected. These cases have all been filed under the habeas data regime.

iii Private litigation

As stated above, the judicial remedy for private plaintiffs is the habeas data procedure regulated by the National Constitution and the Data Protection Law. Despite the fact that the access right of data owners can also be exercised through an administrative procedure, a judicial action is the only way for private plaintiffs to receive financial compensation.

Considering that the administrative procedure before the Data Protection Agency is a fast, free and accessible mechanism, there are not many cases brought at the judicial level.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Unlike most recent European legislation and the regulations contained in the Draft, the Data Protection Law does not specifically regulate international jurisdiction. The Data Protection Agency has no enforcement authority under the current regime regarding companies that are based abroad with no assets or registrations in Argentina, even if these companies collect and treat personal data from Argentine residents. However, foreign companies registered in or that have assets in Argentina must register with the Data Protection Agency and register their databases, to comply with the Argentine data protection regime.

Consequently, on a theoretical level, what triggers the need to comply with the Argentine regime for personal data protection is the collection or treatment of personal
data from Argentine residents. On a practical level, the need to comply with Argentine regulations is triggered by the presence of the foreign company in Argentina by way of assets or registrations in the Public Registry of Commerce.

A few months ago, a well-known technology and transport company started offering its services in Argentina, opening offices and hiring personnel. Because of the media coverage its services received, it came to the Data Protection Agency’s attention that the company was operating through mobile applications that necessarily collected data, but no databases were registered. For that reason, the Data Protection Agency started an investigation and required the foreign company to register its databases with the Data Protection Agency.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity is not a highly regulated area in Argentina. The Data Protection Law does not contain specific regulations regarding data breaches. There are some regulations enacted by the National Central Bank regarding data security obligations for financial institutions, but there is no uniform or omnibus legislation that regulates the matter.

Although Resolution No. 580/2011 of the Chief of Staff created the National Programme for Critical Infrastructures for Information and Cybersecurity, there are not many companies taking part in this programme as it is not mandatory. Its main aim is to promote the creation and adoption of a specific regulatory framework for the protection of strategic infrastructures for the national public sector, inter-jurisdictional organisations and private sector organisations that require it. It seeks the collaboration of those sectors to develop adequate strategies and structures for coordinated action.

Furthermore, Decree 577/2017 has created the Cybersecurity Committee, which will mainly focus on creating a regulatory framework, educating people on the importance of cybersecurity, creating a national cybersecurity plan and creating general guidelines for security breaches. The Ministries of Modernisation, Defence and Security will take part in this initiative.

X OUTLOOK

The future landscape in Argentina regarding personal data protection includes the almost certain enactment of a new law, in line with the new technologies that have emerged since the year 2000.

It is not certain whether the Draft will be sent to Congress and finally passed, but it is the first stepping stone and is certainly one of the Data Protection Agency’s objectives. We believe that a new law, in line with the European Union General Data Protection Regulation, will be enacted within the next two years.

Another probable, significant change in the near future is the creation of a new autonomous and independent enforcement agency, operating outside the scope of the Ministry of Justice. The lack of an autonomous enforcement authority has been a matter of criticism in the international community and many believe that, if it is not solved in the near future, it may lead to the loss of Argentina’s status as an ‘adequate’ country by EU standards regarding data protection.
Chapter 5

AUSTRALIA

Michael Morris

I OVERVIEW

The principal legislation protecting privacy in Australia is the federal Privacy Act 1988 (the Privacy Act). The Privacy Act establishes 13 Australian privacy principles (APPs), which regulate the handling of personal information by many private sector organisations and by federal government agencies.

The body responsible for enforcing the Privacy Act is the Office of the Australian Information Commissioner (OAIC). In practice, the Information Commissioner (the Commissioner) is responsible for the majority of the privacy-related functions of the OAIC, including the investigation of complaints made by individuals.

Substantive amendments to the Privacy Act came into effect on 12 March 2014. In particular, from that date, substantial monetary penalties (currently, up to A$420,000 for individuals or A$2.1 million for corporations) can now be imposed for ‘serious’ or ‘repeated’ interferences with the privacy of individuals.

Although this chapter is principally concerned with the Privacy Act, each Australian state and territory has also passed legislation that protects information held about individuals by state and territory government organisations.

Privacy also receives some protection through developments to the common law, particularly developments in the law relating to confidential information. However, to date the Australian courts have not recognised a specific cause of action to protect privacy, although there has been judicial suggestion that such a development may be open.

There is no general charter of human rights in Australia, and as such there is no general recognition under Australian law of privacy being a fundamental right.

II THE YEAR IN REVIEW

According to the OAIC’s Annual Report 2015–16 (the most recent report as at 11 September 2017), the OAIC received 2,128 privacy complaints and responded to 19,092
privacy enquiries in the year ending 30 June 2016. The Commissioner also initiated 17 investigations, worked on 21 assessments and received 107 voluntary data breach notifications from organisations.

Although there have been several significant enforcement actions (see Section VII for more information), no monetary penalties have yet been imposed on organisations under the new sanction provisions.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

General

The Privacy Act protects personal information – that is, information or an opinion about an identified individual or an individual who is reasonably identifiable. Special protection is afforded to ‘sensitive information’ (see further discussion below).

The Privacy Act contains exemptions for certain organisations from the requirement to comply with the APPs. Operators of small businesses (businesses with an annual turnover for the previous financial year of A$3 million or less) are not generally subject to the Privacy Act.6 There are also exemptions for domestic use,7 media organisations8 and political representatives.9 There is no general exemption for not-for-profit organisations.

There is a broad exemption10 from the application of the Privacy Act for acts or practices that are directly related to a current or former employment relationship and that involve an employee record held by the employer. In practice, this means that many activities of organisations with respect to their own employees are exempted from the Privacy Act.

There is a limited exemption from the application of the Privacy Act for the sharing of personal information (other than sensitive information) between companies in the same corporate group.11 The rules regarding the disclosure of personal information outside Australia apply even where the information is shared between group companies.

Protection of sensitive information

Sensitive information is defined in Australia as being:

Information or an opinion about an individual’s:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;

---

6 Section 6D.
7 Section 16 of the Privacy Act.
8 Section 7B(4) of the Privacy Act.
9 Section 7C(1) of the Privacy Act.
10 Section 7B(3) of the Privacy Act.
11 Section 13B of the Privacy Act.
Generally, an organisation must not collect sensitive information about an individual unless the individual has consented to the collection and the personal information is reasonably necessary for one or more of the organisation’s functions or activities. An organisation may collect sensitive information about an individual without consent in certain limited circumstances; for example, where collection is required by Australian law.

**APP Guidelines (Guidelines)**

The OAIC has published Guidelines to assist organisations in complying with the APPs. Although the Guidelines are not legally binding, they provide guidance as to how the APPs will be interpreted and applied by the Commissioner when exercising his or her functions and powers under the Privacy Act.

**ii General obligations for data handlers**

There is no distinction in the Privacy Act between entities that control and those that process personal information. Any handling of personal information, whether holding, processing or otherwise, is potentially subject to the APPs. The 13 APPs are summarised below.

**APP 1 – open and transparent management of personal information**

Organisations must take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. See the discussion on the required content of privacy policies in Section V.

**APP 2 – anonymity and pseudonymity**

Individuals must have the option of not identifying themselves unless this is impracticable.

**APP 3 – collection of solicited personal information**

Information may be collected only if it is reasonably necessary for the organisation’s functions or activities and must be collected only by lawful and fair means. An organisation may only collect information directly from the individual, unless this is unreasonable or impracticable.

**APP 4 – unsolicited personal information**

Where an organisation receives unsolicited personal information, it must, within a reasonable period, determine whether it could have collected the information itself under the APPs. If not, the organisation must destroy or ‘de-identify’ that information.
APP 5 – notification of collecting personal information

At or before the time of collection (or as soon as practicable afterwards), an organisation collecting personal information must take such steps (if any) as are reasonable in the circumstances to make the individual aware of a number of prescribed matters; for example:

a the identity of the organisation;
b the purposes of the collection;
c the types of organisation to whom the personal information may be disclosed;
d whether the organisation is likely to disclose the information to overseas recipients (and, if so, to which countries); and
e that the organisation’s privacy policy contains certain information (e.g., how to make a complaint).

Where personal information is not collected directly from the individual, an organisation must take reasonable steps to make sure the individual is informed of the same matters in respect of its indirect collection.

APP 6 – uses or disclosures of personal information

Personal information must only be used or disclosed for the purpose for which it was collected (the primary purpose). Personal information may be used or disclosed for a secondary purpose where:

a the secondary purpose is related to the primary purpose and the individual would reasonably expect it to be disclosed or used this way;
b the individual has consented to that disclosure or use; or
c another exception applies (e.g., that the use or disclosure is required by Australian law).

In the case of sensitive information, the secondary use or disclosure under item (a) above must be directly related to the primary purpose.

APP 7 – direct marketing

Sensitive information can only ever be used for direct marketing with the individual’s consent. Other personal information cannot be used or disclosed for direct marketing unless an exception applies. Where direct marketing is permitted, organisations must always provide a means for the individual to ‘opt out’ of direct marketing communications.

APP 7 does not apply to the extent that the Do Not Call Register Act 2006 (Cth) or the Spam Act 2003 (Cth) apply.

APP 8 – cross-border disclosure of personal information

APP 8 regulates the disclosure of information to a person who is outside Australia. See the discussion in Section IV for further details of the requirements of APP 8.

Under Section 16C of the Privacy Act, in certain circumstances, an organisation may be deemed to be liable for a breach of the APPs by an overseas recipient of personal information disclosed by that organisation.
APP 9 – adoption, use or disclosure of government-related identifiers
An organisation must not adopt an identifier that has been assigned to an individual by a government agency as its own identifier of the individual; or disclose or use an identifier assigned to an individual by a government agency, unless an exception applies (e.g., the adoption, disclosure or use is required or authorised by an Australian law).

An identifier includes things such as a driving licence and passport number.

APP 10 – quality of personal information
An organisation must take reasonable steps to ensure that the personal information it collects, uses and discloses is accurate, complete and up to date and also, in the case of use or disclosure, relevant.

APP 11 – security of personal information
Organisations must take reasonable steps to protect information they hold from misuse, interference, loss, unauthorised access, modification or disclosure; and destroy or de-identify information once it is no longer needed for any purpose for which the information may be used or disclosed under the APPs.

APP 11 does not mandate any specific security obligations or standards. The OAIC, however, has published a Guide to securing personal information, which provides non-binding guidance on the reasonable steps organisations are required to take to protect the personal information they hold.

There are no specific rules governing the handling of personal information by third parties. The obligation placed on organisations under APP 11 to take reasonable steps to protect personal information they hold has the effect of requiring organisations to take reasonable steps to ensure that any third party (including an overseas data processor) handling personal information on their behalf also takes reasonable steps to protect personal information. The above-mentioned Guide to information security also provides non-binding guidance in relation to the processing of information by third parties.

APP 12 – access to personal information
As a general rule, an organisation must, upon request, give an individual access to any personal information held about him or her. There are exceptions to this general rule, including where the provision of access to personal information could have an unreasonable impact on the privacy of other individuals, or where denying access is required or authorised by Australian law.

APP 13 – correction of personal information
An organisation must take reasonable steps to correct any personal information if the entity is satisfied the information is inaccurate or where the individual requests the entity to do so. According to the Guidelines, the reasonable steps to be taken may include ‘making appropriate [. . .] deletions’. However, individuals do not have an express legal right to have inaccurate data deleted.

If an organisation refuses to correct personal information, it must give reasons to the person who has requested the correction and tell them about the mechanisms available to complain about the refusal.

iii Technological innovation and privacy law

The Privacy Act is drafted in a technologically neutral manner and its provisions can be applied to developments in new technologies. As an example, the direct marketing principle, APP 7, has been taken by the Commissioner\(^\text{13}\) to apply to online behavioural advertising (OBA). In consequence, the requirements of APP 7 (e.g., to allow people to opt out of marketing communications) could apply to advertisements appearing through use of OBA.

As another example, although Australia does not have any specific ‘cookie’ legislation, the collection of data through the use of cookies could amount to the collection of personal information if the individual’s identity is known or able to be reasonably determined by the collector. In those circumstances, the requirements of the APPs with respect to the information will apply accordingly.

Since sensitive information under the Privacy Act includes biometric information that is used for the purpose of automated biometric identification, it is likely that the use of automated facial and speech recognition technologies will require compliance with the obligations of the APPs relating to sensitive information. Those obligations include the requirement to obtain consent before the relevant biometric information is collected.

iv Specific regulatory areas

There are a number of state and federal acts that protect privacy in particular circumstances, such as when communicating over a telecommunications network, accessing a computer system, or when engaging in activities in a private setting or that protect specific types of information, such as credit information, tax file numbers, healthcare identifiers, eHealth records or health records.

IV INTERNATIONAL DATA TRANSFER

APP 8 provides that, prior to disclosing personal information to a recipient who is located outside Australia, an organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the personal information. This requirement does not apply if:

\[\begin{align*}
\text{a} & \quad \text{the organisation reasonably believes that the overseas recipient is bound by a law similar to the APPs that the individual can enforce;} \\
\text{b} & \quad \text{the individual consents to the disclosure of the personal information in the particular manner prescribed by APP 8; or} \\
\text{c} & \quad \text{another exception applies (e.g., that the disclosure of the personal information is required by Australian law).}
\end{align*}\]

The consent required by APP 8 has to be an informed consent and in many cases its requirements are likely to be difficult to satisfy in practice. Further, in many cases the overseas recipient will not be subject to a similar overseas law that is enforceable by the individual. Accordingly, in most cases, the organisation must take ‘reasonable steps’ to ensure that the overseas recipient does not breach the APPs prior to disclosing that information to the overseas recipient. The Guidelines indicate that taking reasonable steps usually involves the organisation obtaining a contractual commitment from the overseas recipient that it will handle the personal information in accordance with the APPs.

V COMPANY POLICIES AND PRACTICES

APP 1.3 requires organisations to have a clearly expressed and up-to-date policy about their management of personal information. An organisation is required to take such steps as are reasonable in the circumstances to make its privacy policy available free of charge and in such a form as is appropriate. This will generally involve the organisation making its privacy policy available on its website.

Aside from the general obligation to include information about the management of personal information, the privacy policy must contain the following specific information:

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

The Commissioner has published in its Guidelines further information as to its expectations with respect to the contents of the privacy policy.

Aside from the specific obligation to have and maintain a privacy policy, APP 1.2 requires an organisation to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the organisation’s functions or activities that will ensure that the organisation complies with the APPs.

This is an overarching obligation applying to organisations in Australia and is generally understood as requiring organisations in Australia to implement the principles of ‘privacy by design’. Helpful guidance as to what the Commissioner expects organisations to do to comply with this general obligation was published by the Commissioner in May 2015.14

VI DISCOVERY AND DISCLOSURE

Under APP 6, in general personal information can only be used and disclosed for the purpose for which the information was collected or for a related secondary purpose that would be reasonably expected by the individual. The disclosure of information in response to national or foreign government requests, or in response to domestic or foreign discovery court orders or internal investigations, would not normally satisfy this requirement. However, there are a number of exceptions that may, depending on the circumstances, be available to allow disclosure in response to such requests or orders. These are summarised below.

In the case of Australian legal proceedings, APP 6.2(b) allows disclosure if the disclosure is ‘required or authorised by or under an Australian law or a court/tribunal order’. This will allow disclosures that are required or authorised under Australian rules of court.

In addition, Section 16A(i)(4) of the Privacy Act allows disclosure where it is ‘reasonably necessary for the establishment, exercise or defence of a legal or equitable claim’. Disclosures of information in the course of legal proceedings where the disclosures are necessary to either assert or defend a claim will accordingly be permitted. Section 16A(i)(5) allows disclosure where it is reasonably necessary for the purposes of a ‘confidential alternative dispute resolution process’. This will permit disclosures in the course of confidential mediations and the like. However, these exceptions do not apply to the disclosure of information to someone outside Australia and so would not be available for claims being pursued in foreign courts.

To disclose information in response to the order of a foreign government or court the disclosure will have to comply with both APP 6 and APP 8 (the cross-border disclosure principle). There has been no binding Australian legal decision on the consequences of a person receiving in Australia an order from a foreign court requiring the disclosure of personal information outside Australia. To satisfy both APP 6 and APP 8, the party seeking disclosure of the information outside Australia is likely to have to apply under a relevant international treaty (such as the Hague Convention), to which Australia is a party and which has been implemented in Australian local law. If these conditions can be satisfied, then the disclosure of the information outside Australia will be ‘required or authorised by or under an Australian law’ and so will be permitted under both APP 6.2(b) and APP 8.2(c).

Another option that might be available in some circumstances would be to redact all personal information from the relevant document before the document is disclosed outside Australia. Whether a document that has been redacted in this way will still comply with the orders of the foreign court will depend on the circumstances.

With respect to disclosures outside Australia, Section 13D(1) provides that acts done outside Australia do not interfere with privacy if the act is required by an applicable law of a foreign country. This exception may be of use where relevant personal information is already located outside Australia and, pursuant to the legal process in the place where it is located, it has to be disclosed to someone in that place. The exception will not be available with respect to information that is located in Australia.
VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

If an individual makes a privacy complaint, the Commissioner has the power to attempt, by conciliation, to effect a settlement of the matter or to make a determination that includes declarations that:

a the individual is entitled to a specified amount as compensation for loss or damage suffered (including for injury to feelings or for humiliation);

b the organisation has engaged in conduct constituting an interference with the privacy of an individual and that it must not repeat or continue the conduct; and

c the organisation perform any reasonable act or course of conduct to redress any loss or damage suffered by the individual.

A determination of the Commissioner regarding an organisation is not binding or conclusive. However, the individual or the Commissioner has the right to commence proceedings in court for an order to enforce the determination.

The Commissioner also has the power to audit organisations (these audits are referred to in the Privacy Act as 'assessments'), accept enforceable undertakings, develop and register binding privacy codes and seek injunctive relief in respect of contraventions of the Privacy Act.

Finally, the Commissioner may apply to the Federal Court or Federal Circuit Court for a penalty (currently, up to A$420,000 for individuals or A$2.1 million for corporations) to be imposed for ‘serious’ or ‘repeated’ interferences with privacy. These penalties constitute regulatory fines and cannot be used to compensate individuals for breaches of the Privacy Act. As noted above, the Commissioner has not yet sought to levy the penalty on any organisation.

ii Recent enforcement cases

The Commissioner has recently taken action in a number of significant cases that are of potentially broad interest. These are summarised below.

Enforceable undertaking from Avid Life Media (ALM) following website attack

One of the enforcement powers available to the Commissioner is to accept an enforceable undertaking from an organisation it is investigating for breaches of privacy. Such an undertaking is likely to be offered by the organisation in the course of resolving an investigation by the Commissioner into its activities. The undertakings are enforceable by the Commissioner in the Federal Court.

ALM operates a number of adult dating websites, including ‘Ashley Madison’. It is based in Canada, but its websites have users around the world, including Australia.

In July 2015, a cyber attacker announced the ALM website had been hacked and threatened to expose the personal information of Ashley Madison users unless ALM shut down its controversial website. ALM did not agree to the demand and, as a consequence, information that the hacker claimed was stolen from ALM (including profile information, account information and billing information from approximately 36 million user accounts) was published. This prompted the Commissioner and the Office of the Commissioner of Canada to launch a joint investigation into ALM’s privacy practices.

The OAIC was satisfied that ALM was an organisation with an Australian link as it carried on business and collected personal information in Australia (despite not having
a physical presence in Australia). The investigation identified a number of contraventions of the APPs, including with regard to ALM’s practice of indefinite data retention and ALM not having an appropriate information security framework in place.

The Commissioner accepted an enforceable undertaking from ALM to address the concerns identified.

**Provision of an enforceable undertaking by Optus**

On 27 March 2015, the Commissioner accepted an enforceable undertaking from Optus (a major Australian telecommunications company) arising out of its investigation into three privacy incidents involving Optus.

In the first of these incidents, Optus became aware in April 2014 that, because of a coding error, the names, addresses and phone numbers of 122,000 Optus customers were listed in the White Pages directory without those customers’ consent. In the second incident, Optus had issued modems to its customers in such a way that the management ports for the modems were issued with user default names and passwords in place. The consequence was that Optus customers who did not change the default user names and passwords were then vulnerable to a person making and charging calls as though they were the Optus customer. However, there was no evidence that the vulnerability had in fact been exploited. The final incident involved a security flaw that left some Optus customers vulnerable for eight months to ‘spoofing attacks’, under which an unauthorised party could access a customer’s voicemail account.

Following an eight-month investigation, the Commissioner concluded that an enforceable undertaking was the most appropriate regulatory enforcement action in the circumstances. This conclusion was due, in most part, to Optus’ cooperation with the Commissioner and steps it had taken to respond to the Commissioner’s concerns. Under the terms of the undertaking, Optus was required to appoint an independent third party to conduct reviews of the additional security measures Optus adopted in response to the privacy incident and its vulnerability detection processes concerning the security of personal information.

**Metadata collected by telecommunications companies constituted personal information to which the relevant individual could obtain access**

In May 2015, the Commissioner found that metadata could be personal information under the Privacy Act where the organisation holding that data has the capacity and resources to link that information to an individual. The background to that finding was a request made by a journalist to access all metadata that Telstra (Australia’s largest telecommunications company) stored about him in relation to his mobile service. Over the course of some months, Telstra ultimately released much of the requested metadata to the journalist, but continued to refuse access to IP address information, URL information and cell tower location information beyond that which Telstra retained for billing purposes.

The Commissioner found that the above three categories of information did constitute personal information under the Privacy Act and that Telstra had breached the Privacy Act by failing to release that information.

The decision was overturned by the Administrative Appeals Tribunal (AAT) in December 2015. The AAT reasoned that mobile network data would need to be information ‘about an individual’ for it to fall within the definition of personal information. It found that the relevant mobile network data was not information about an individual as such, but rather
information about the way in which Telstra delivers its services. It could not, therefore, be
classified as personal information under the Privacy Act and did not need to be disclosed
to customers upon request.

In coming to the conclusion that the mobile network data was not personal information,
the AAT appears to have been influenced by evidence from Telstra that its mobile network
data were kept separate and distinct from customer databases, rarely linked to these databases
and not ordered or indexed by reference to particular customers.

On 14 January 2016, having considered the AAT’s decision, the Commissioner filed
a notice of appeal from a tribunal to the Federal Court of Australia. The Federal Court
dismissed the Commissioner’s appeal on 19 January 2017. In dismissing the appeal, the
Court confirmed that if information is not ‘about an individual’, the information will not be
personal information and, accordingly, the Privacy Act will not apply.

Enforceable undertaking from the Australian Red Cross following inadvertent disclosure
by a third-party contractor

On 5 September 2016, a file containing personal information of approximately 550,000
individuals was inadvertently posted to a publicly accessible section of the Australian Red
Cross (the Red Cross) website by a third-party contractor. This included ‘personal details’ and
identifying information such as names, gender, addresses and sexual history.

The Red Cross was only made aware of this breach after an unknown individual notified
the Red Cross through multiple intermediaries on 25 October 2016. Upon notification, the
Red Cross took a number of immediate steps to contain the breach. This included notifying
affected individuals, undertaking a risk assessment of the information compromised and
conducting a forensic analysis on the exposed server.

The Commissioner found that the Red Cross did not breach the obligation relating to
unauthorised disclosure of personal information, as it did not disclose personal information,
this was done by a third-party employee. In addition, it was found that although the
Red Cross did not physically hold the personal information, it retained ownership of the
information because of the terms of its contract with the third-party contractor. Because of
its ownership of the personal information, the Red Cross had an obligation to protect this
personal information against unauthorised access or disclosure. The Commissioner concluded
that the Red Cross had breached this obligation by failing to properly assess the adequacy
of its third-party contractor’s security practices and by failing to include control measures to
mitigate the risks of contracting with a third party in its contractual arrangements.

The Red Cross accepted an enforceable undertaking on 28 July 2017 to engage
an independent review of its third-party management policy and standard operating
procedure. The third-party contractor also entered into an enforceable undertaking with
the Commissioner’s office to establish a data breach response plan and update its data
protection policy.
iii Private litigation

In general, privacy legislation is only enforceable in Australia by the relevant authority. However, some limited private rights of action do exist, particularly a general right under the Privacy Act for anyone to seek an injunction to restrain conduct that would be a contravention of the Act.¹⁵

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Privacy Act has a broad extraterritorial application and applies to the overseas activities of Australian organisations and foreign organisations that have an ‘Australian link’.¹⁶

An organisation is considered to have an ‘Australian link’ if there is an organisational link¹⁷ – for example, the organisation is a company incorporated in Australia; or if the organisation carries on business in Australia and collects or holds personal information in Australia.¹⁸ This has been interpreted very broadly as including an organisation that has a website that offers goods or services to countries including Australia.¹⁹

If an organisation’s overseas activity is required by the law of a foreign country, then that activity is not taken to amount to an interference with the privacy of an individual.²⁰

IX CYBERSECURITY AND DATA BREACHES

As stated above, APP 11 requires an organisation to take such steps as are reasonable in the circumstances to protect information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

The obligation in APP 11 would extend to taking reasonable steps to protect information that an organisation holds against cyberattacks. See the discussion on APP 11 in Section III for more details of its requirements.

In addition to the general obligation under APP 11, particular industry sectors are subject by their regulators to take additional measures to protect information (including personal information) that they hold. Government agencies are also generally subject to government-specific security requirements, most notably the Protective Security Policy Framework.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 received royal assent on 22 February 2017 and will come into effect no later than 12 months after this date. The Privacy Amendment Act amends the Privacy Act to impose an express obligation on entities to notify the OAIC, affected individuals and at-risk individuals in the event of an ‘eligible data breach’.

An eligible data breach refers to any unauthorised access, disclosure or loss of information that a ‘reasonable person’ is ‘likely’ to conclude would result in serious harm to an individual. In the event an entity becomes aware that an eligible data breach may have

¹⁵ Section 98 of the Privacy Act.
¹⁶ Section 5B(1A) of the Privacy Act.
¹⁷ Section 5B(2) of the Privacy Act.
¹⁸ Section 5B(3) of the Privacy Act.
²⁰ Section 13D(1) of the Privacy Act.
occurred, it must provide a copy of a statement to the OAIC setting out the details of the breach as soon as is practicable. It must also subsequently notify any individuals affected by or at risk of being affected by the eligible data breach.

X    OUTLOOK

On 31 August 2017, the OAIC released its Corporate Plan 2017–2018. 21 The Corporate Plan indicates that the OAIC will focus on the following activities in the coming year: preparing for the implementation of the Notifiable Data Breaches scheme; conducting targeted privacy audits (assessments) in areas of national security, national health and identity management to assess organisations’ compliance with the Privacy Act; and the development of an Australian Public Services Privacy Governance Code.

Chapter 6

BELGIUM

Steven De Schrijver

I OVERVIEW

The Belgian legislative and regulatory approach to privacy, data protection and cybersecurity is quite comprehensive. The most important legal provisions can be found in the following:

a. Article 22 of the Belgian Constitution, which provides that everyone is entitled to the protection of his or her private and family life;

b. the Act of 8 December 1992 on Privacy Protection in Relation to the Processing of Personal Data (the Data Protection Act), further implemented by the Royal Decree of 13 February 2001;


d. the Act of 13 June 2005 on Electronic Communications (the Electronic Communications Act); and

e. the Act of 28 November 2000 on Cybercrime.

Because of a series of cybersecurity attacks on a number of banks and private companies in the past few years, cybersecurity has increasingly received more and more attention in Belgium in recent years. One of Belgium’s most notable cybersecurity incidents, however, was the lightning strike in 2015 at the Google data centre in Mons, which was struck four times during a summer storm, resulting in permanent data loss on a tiny fraction (0.000001 per cent) of the total disk space.

Since presenting its national cybersecurity strategy in 2012, Belgium has made substantial efforts to enhance cybersecurity. For instance, a secret Belgian operation in 2016 prevented the worldwide cyberattacks by the WannaCry ransomware virus from causing large-scale damage in Belgium in 2017. The Centre for Cybersecurity Belgium (CCB) had collected data from the global IT security company Rapid7 on Belgian companies’ cybersecurity in 2016 after the country scored badly in Rapid7’s National Exposure Index report that year, and used this information to warn companies. In 2017, Belgium is now ranked as the 179th most exposed country of 183 countries, in comparison with 2016, when it was ranked first, and therefore the most exposed country.

Furthermore, while the NotPetya ransomware virus did cause some damage within multinationals in Belgium, the federal cyber-emergency team (CERT) reports that efforts made after the WannaCry ransomware attack have paid off, as the damage in Belgium was limited. The responsibilities of the CCB and CERT are discussed further in Section IX.

1 Steven De Schrijver is a partner at Astrea.
Belgium is now looking to also improve cybersecurity in the military field, with the Belgian army recruiting 92 computer experts in 2017, and planning to recruit up to 200, to form a ‘cyber-army’ responsible for protecting possible military targets.

II  THE YEAR IN REVIEW

Last year’s most heated debate concerned the case against Facebook initiated by the Belgian Privacy Commission (Belgium’s data protection authority (DPA)) in relation to Facebook’s use of ‘social plug-ins’ to track the internet behaviour of not only its users, but also internet users without a Facebook account at all. The case still continues, although the interim measures imposed on Facebook by the President of the Court of First Instance have been overruled at appeal on jurisdictional grounds and, because of a lack of urgency, we are still awaiting a final ruling on the merits of the case, which is expected to be delivered at the end of 2017. This year, however, the focus has been on the ongoing discussion about whether foreign internet service providers, such as Yahoo! or peer-to-peer internet software providers such as Skype, are to be considered electronic communications service providers under Belgian law and subject to the jurisdiction of the Belgian courts.

After the final judgment in the Yahoo! saga on 1 December 2015, in which the Belgian Supreme Court dismissed an appeal lodged by Yahoo! against the ruling of the Court of Appeal of Antwerp obliging Yahoo! to disclose to the Belgian judicial authorities (despite the fact that Yahoo! had no establishment or personnel in Belgium) the identity of persons who committed fraud via its email service, the Court of First Instance of Mechelen had to rule on Skype’s duty not only to disclose certain information, but also to provide technical assistance for the interception of the content of ‘live’ voice communications. Whereas the obligation to disclose information (and thus jurisdiction) could be located in Belgium in the Yahoo! case on the grounds of the ‘portability’ of information, this reasoning was difficult to apply by analogy to technical assistance that had to be provided in Luxembourg because Skype is a Luxembourg company and has no infrastructure in Belgium, and this would require material acts abroad. Nonetheless, the Court of First Instance imposed a fine of €30,000 on Skype for its refusal to cooperate in setting up a wiretap ordered by the Mechelen investigative judge. The Court ruled that the technical assistance required of Skype was to be extended in Belgium and the technical impossibility of Skype cooperating was irrelevant because Skype itself had created this impossibility by organising its operations in the way it did. Skype lodged an appeal against this judgment with the Court of Appeal of Antwerp, which is expected to deliver its judgment by the end of 2017 (see Section VI).

Another judgment that caused considerably controversy in the past year was the ruling of the Belgian Supreme Court of 13 December 2016, which declared unlawful all speeding tickets issued by the police solely on the basis of number plate identification (using roadside cameras). The Supreme Court found that the police had never been granted formal authorisation to retrieve personal information of the alleged traffic offenders from the database of the Vehicle Registration Service (DIV), where the names and addresses of all car owners are collated with the record of their number plates. The Supreme Court concluded that the police were therefore in violation of the Data Protection Act and fines imposed illegally through the use of unlawfully obtained personal data could be challenged and reviewed in court. However, the police authorities solved this illegality issue very quickly by applying for and being granted a formal authorisation from the DPA to consult the DIV database for identification purposes. This case clearly demonstrates that the Belgian
judiciary acknowledges the importance of privacy legislation in modern-day life and that even government bodies have to face the consequences of any non-compliance with privacy and data protection legislation.

Privacy-related concerns also arose with respect to the implementation of the low-emission zone (LEZ) in Antwerp, prohibiting polluting vehicles from entering the city centre, to improve the air quality of the city. The City of Antwerp placed smart cameras equipped with an automated number plate recognition system at the boundaries of the LEZ and a LEZ database was created, the data in which were mainly retrieved from the DIV, including a whitelist of compliant vehicles. Initially, the DPA considered that, by duplicating the entire DIV database in the LEZ database, the City of Antwerp was violating the proportionality principle set out in the Data Protection Act as the personal data of all vehicle owners registered in Belgium would be duplicated, while only a limited number of these vehicles would enter the LEZ zone. Subsequently, in June 2016, an adapted version of the project was submitted and accepted by the DPA, because it had limited the content of the LEZ database and put extra security measures in place.

Lastly, on 22 December 2016, the Court of Justice of the EU (CJEU) ruled that the statutory retention period of one year for metadata held by telecom operators and electronic communication service providers laid down in the recently amended Act of 13 June 2005 on Electronic Communications (amended by the Act on Data Retention of 29 May 2016) is incompatible with the right to privacy of individuals. The retention obligation should be limited to what is strictly necessary for the purposes the authorities want to achieve. The CJEU held that in the fight against ‘serious crime’, EU Member States are allowed to retain data in a targeted manner and only after review by a court or independent body, except in very urgent cases. We will have to wait and see what effect the CJEU ruling will have on this new Belgian data retention legislation.

III  REGULATORY FRAMEWORK

i  Privacy and data protection legislation and standards

The Belgian privacy and data protection legislation is set forth in the Act of 8 December 1992 on privacy protection in relation to the processing of personal data (the Data Protection Act). This Act was amended by the Act of 11 December 1998 with a view to implementing the provisions of the EU Data Protection Directive (which will of course be replaced by the new EU General Data Protection Regulation (GDPR), which entered into force on 24 May 2016 and will apply as of 25 May 2018).

Belgium has transposed the EU Data Protection Directive quite literally, so the definitions of the different concepts, such as personal data, sensitive personal data and data controllers, are identical or very similar to the definitions used in EU law. As such, ‘personal data’ means any information relating to an identified or identifiable natural person whereby an ‘identifiable person’ is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her identity. ‘Sensitive personal data’ means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health, sex life or judicial information.
The data controller is the person who alone or jointly with others determines the purposes and means of the processing of personal data, and data processors are persons that process personal data on behalf of a data controller. Under Belgian law, it is also possible for different persons or entities to act as data controller in respect of the same personal data.

The Belgian enforcement agency with responsibility for privacy and data protection is the DPA. The DPA’s mission includes monitoring compliance with the provisions of the Data Protection Act, but it cannot impose any administrative penalties upon individuals or organisations. However, the GDPR has broadened the powers of the DPA. As of mid-2018, the DPA will have increased investigative powers, the right to initiate legal proceedings as well as the right to impose interim measures and administrative fines.

The Data Protection Act provides for criminal sanctions for most provisions, including the duty to inform the data subject and the duty to file a prior notification of processing operations to the DPA. Penalties range from €600 to €600,000 and include, in specific cases, imprisonment of up to two years. The publication of a judgment may also be ordered, together with other measures that may constitute a serious threat to the data controller, such as confiscation of the support media, an order to erase the data or a prohibition on using the personal data for up to two years. There is no requirement to establish any harm or injury as a result of a breach of the Data Protection Act for the sanctions to apply, but obviously the existence of such harm or injury may have an impact on the judicial authorities’ decision whether to prosecute.

ii General obligations for data handlers

Data controllers must notify the DPA of any automated data processing operation. Such a notification is a mere filing and can be done by filling in an online form and submitting a signed copy to the DPA. Any changes to the data processing operation must also be notified. Notification is only required for automated processing (and not for manual files) with certain limited exemptions (e.g., payroll and personnel administration, accounting and client or supplier administration).

Non-sensitive personal data may be processed if the processing is:

a carried out with the data subject’s consent;
b necessary for the performance of a contract with the data subject;
c necessary for compliance with a legal obligation;
d necessary to protect the vital interests of the data subject;
e necessary for the public interest or in the exercise of official authority; or
f necessary for the data controller’s or recipient’s legitimate interests, except where overridden by the interests of the data subject.

In addition, the processing must comply with the general principles of data processing, which implies that personal data is to be:

a processed fairly and lawfully;
b collected for specific, explicit and legitimate purposes, and not processed in a manner incompatible with those purposes;
c adequate, relevant and not excessive;
d accurate and, where necessary, up to date; and
e kept in an identifiable form for no longer than necessary.
Sensitive personal data (i.e., personal data related to racial or ethnic origin, sexual orientation, religious or political beliefs, union membership, or health or judicial information) may only be processed if the processing:

a. is carried out with the data subject’s explicit written consent;
b. is necessary for a legal obligation in the field of employment law;
c. is necessary to protect the vital interests of the data subject where the data subject is unable to give consent;
d. is carried out by a non-profit body and relates to members of that body or persons who have regular contact with it;
e. relates to data made public by the data subject;
f. is necessary for legal claims; or
g. is necessary for medical reasons.

In practice, the legitimate interest condition is frequently relied upon as a ground for processing non-sensitive personal data. It should be noted, however, that the DPA finds that obtaining the unambiguous consent of the data subject is best practice and that the legitimate interest condition is only a residual ground for processing.

Except with respect to the processing of sensitive personal data, where consent of the data subject must be provided in writing, Belgian law does not impose any formalities regarding obtaining consent to process personal data. Such consent may be express or implied, written or oral, provided it is freely given, specific and informed. However, as consent should be unambiguous as well, it is recommended to obtain express and written consent for evidential purposes.

With respect to the processing of employees’ personal data, the DPA finds that such processing should be based on legal grounds other than consent, in particular the performance of a contract with the data subject, since obtaining valid consent from employees is considered difficult (if not impossible) given their subordinate relationship with the employer.

As far as the data subjects’ right of access, correction and removal is concerned, Belgian law provides that a data controller must provide a data subject access to his or her data upon request and free of charge. The data subject has the right to have inaccurate data corrected or deleted and, in certain cases, he or she may object to decisions being made about him or her based solely on automatic processing. To exercise this right, the data subject must send a dated and signed request to the data controller, who must confirm the amendment or deletion within one month to the data subject and, where possible, to the third parties to whom the incorrect data was communicated. If the data are to be used for direct marketing purposes, the data subject also has the right to object, free of charge, to the processing and the data controller must inform the data subjects of this right.

iii Specific regulatory areas

Although Belgium has not adopted a sectoral approach towards data protection legislation, there are nevertheless separate regulations in place for certain industries and special (more vulnerable) data subjects. In addition to the Data Protection Act and the Royal Decree of 13 February 2001, specific laws have been adopted to provide additional protection for data subjects in the following sectors:

a. camera surveillance: the installation and use of surveillance cameras is governed by the Camera Surveillance Law of 21 March 2007;
workplace privacy: the installation and use of surveillance cameras for the specific purpose of monitoring employees is subject to Collective Bargaining Agreement No. 68 of 16 June 1998 concerning the camera surveillance of employees. In addition, the monitoring of employees’ online communication is subject to the rules laid down in Collective Bargaining Agreement No. 81 of 26 April 2002 concerning the monitoring of electronic communications of employees.

electronic communications: the Electronic Communications Act of 13 June 2005 contains provisions on the secrecy of electronic communications and the protection of privacy in relation to such communications. Furthermore, the Electronic Communications Act imposes requirements on providers of telecommunication and internet services regarding data retention, the use of location data and the notification of data security breaches;

medical privacy: the Patient Rights Act of 22 August 2002 governs, inter alia, the use of patients’ data and the information that patients need to receive in this respect; and

financial privacy: the financial sector is heavily regulated. For instance, the use of credit card information for profiling violates consumer credit legislation, which clearly states that (1) personal data collected by financial institutions can only be processed for specific purposes, (2) only some data can be collected, and (3) it is prohibited to use the data collected within the credit relationship for direct marketing or prospection purposes. Belgian legislation also requires that information be deleted when its retention is no longer justified.

Noteworthy in an EU context is the fact that jointly with the entry into force of the GDPR, the Network and Information Security Directive (the NIS Directive) should be transposed into national law by the EU Member States by 25 May 2018. In addition to the specific data protection rules above, the NIS Directive will add a legal basis for higher cybersecurity standards in respect of certain ‘essential’ services.

The NIS Directive applies in particular to operators of essential services (OESs). OESs can be found in the following industries:

energy (electricity, oil and gas);
transportation (air, rail, water and road);
banking and financial market infrastructure;
health and drinking water supply and distribution; and
digital infrastructure.

to ensure an adequate level of network and information security in these sectors and to prevent, handle and respond to incidents affecting networks and information systems, the NIS Directive sets out the following obligations for these OESs:

the obligation to take appropriate technical and organisational measures to manage the risks posed to their network and information systems, and to prevent or minimise the impact in the event of a data breach; and

the obligation to notify the competent authority, without undue delay, of all incidents with a ‘significant impact’ on the security of the core services provided by these operators. To assess the impact of an incident, the following criteria should be taken into account: (1) the number of users affected; (2) the duration of the incident; (3) the
geographical spread with regard to the area affected by the incident; and (4) in relation to certain OESs, the disruption of the functioning of the service and the extent of the impact on economic and societal activities.

The notification obligations, preventive actions and sanctions under the NIS Directive should increase transparency regarding network and information security and heighten awareness of cybersecurity risks in the above-mentioned essential services.

iv Technological innovation and privacy law

Cloud computing

In February 2016, the DPA issued advice on the use of cloud computing services (Advice No. 10/2016 of 24 February 2016 on the Use of Cloud Computing by Data Controllers), which set out a number of key principles to be guaranteed in the contractual relationship between data subjects and cloud service providers, *inter alia*, pertaining to legal certainty, confidentiality, data subjects’ rights, data localisation, international data transfer restrictions, data breach notification, government access, technical and organisational information security measures.

Furthermore, the DPA also set out certain guidelines for cloud service providers in their capacity as data controllers, such as: (1) the clear identification of data and data processing activities before migrating the data to the cloud environment, thereby giving due consideration to the nature and sensitivity of the data; (2) contractual and technical requirements for the provision of cloud services; (3) the obligation to identify the most suitable cloud solution; (4) the performance of a risk analysis; and (5) the extension of information to the data subjects about the storage of their personal data in a cloud.

Big-data analytics

The DPA released in March 2017 a report on the use of big data, on which stakeholders could comment until 11 April 2017.

The report aims to reconcile the need for legal certainty with the application of big data in current and future applications, especially in the light of the forthcoming GDPR. The recommendations made in the report cover various aspects, such as data protection compliance and respect for data subjects’ rights. It is not the intention of the DPA to curtail unnecessarily the use of big-data applications as they are often very useful to society. Given that the deadline for comments expired in April, the DPA is expected to take a position and issue a statement on the use of big data soon.

Automated profiling

The DPA has not yet issued any recommendation or opinion on automated profiling. It can be expected, however, that it will take a position similar to the position of the Article 29 Working Party. The Working Party adopted an advice paper on profiling on 13 May 2013, in which it stated that Article 20 of the Data Protection Regulation should be improved by including additional elements to provide for a balanced approach on profiling and mitigate the risks for data subjects. This implies:

a more transparency;

b an increase of the data subjects’ control;
Belgium

c more responsibility and accountability of data controllers; and
d a ‘balanced’ and case-by-case approach taking into account the degree of intrusiveness of a specific processing type or measures on data subjects.

Cookies

The use of cookies is regulated by Article 129 of the Electronic Communications Act, as amended by the Act of 10 July 2012. The latest amendment provides that cookies may only be used with the prior consent of the data subject (i.e., opt-in rather than opt-out consent), who must be informed of the purposes of the use of the cookies as well as his or her rights under the Data Protection Act. The consent requirement does not apply to cookies that are strictly necessary for a service requested by an individual. The user must be allowed to withdraw consent free of charge.

On 4 February 2015, the DPA issued an additional draft recommendation on the use of cookies in which it provided further guidance regarding the type of information that needs to be provided and the manner in which consent should be obtained. This requires an affirmative action by the user, who must have a chance to review the cookie policy beforehand. This policy must detail each category of cookie with their purposes, the categories of information stored, the retention period, how to delete them and any disclosure of information to third parties.

According to the DPA, consent cannot be considered validly given by ticking a box in the browser settings.

In January 2017, the European Commission published the draft text of the new e-Privacy Regulation, which will become directly applicable in Belgium and replace all the current national rules relating to, inter alia, cookies after its adoption in May 2018 (together with the entry into force of the GDPR). The current draft Regulation allows consent to be given through browser settings provided that this consent entails a clear affirmative action from the end user of terminal equipment to signify his or her freely given, specific, informed and unambiguous consent to the storage and access of third-party tracking cookies in and from the terminal equipment. This entails that internet browser providers will have to significantly change the way their browsers function for consent to be validly given via browser settings.

In addition, the proposal clarifies that no consent has to be obtained for non-privacy-intrusive cookies that improve the internet experience (e.g., shopping-cart history) or cookies used by a website to count the number of visitors. Note, however, that this is still a draft text, so it remains to be seen which text will eventually be adopted.

Electronic marketing

Electronic marketing and advertising is regulated by the provisions of Book XII (Law of the Electronic Economy) of the Code of Economic Law, as adopted by the Act of 15 December 2013.

The automated sending of marketing communications by telephone without human intervention or by fax is prohibited without prior consent.

When a company wants to contact an individual personally by phone (i.e., in a non-automated manner) for marketing purposes, it should first check whether the individual is on the ‘do-not-call-me’ list of the non-profit organisation DNCM. Telecom operators
should inform their users about this list and the option to register online. If the individual is registered on the list, the company should obtain the individual’s specific consent before contacting him or her.

Furthermore, the proposal for the new e-Privacy Regulation (already touched on in the context of cookie rules) obliges marketing callers to always display their phone number or use a special prefix that indicates a marketing call. Again, as this is only a draft text, it is not certain that this obligation will effectively be imposed on marketing callers.

Likewise, the use of emails for advertising purposes is prohibited without the prior, free, specific and informed consent of the addressee pursuant to Section XII.13 of the Code of Economic Law. This consent can be revoked at any time, without any justification or any cost for the addressee. The sender must clearly inform the addressee of its right to refuse the receipt of any future email advertisements and on how to exercise this right using electronic means. The sender must also be able to prove that the addressee requested the receipt of electronic advertising. The sending of direct marketing emails does not require consent if they are sent to a legal entity using ‘impersonal’ electronic contact details (e.g., info@company.be). The use of addresses such as john.doe@company.be, however, remains subject to the requirement for prior consent.

Unless individuals have opted out, direct marketing communications through alternative means are allowed. Nonetheless, the Data Protection Act prescribes a general obligation for data controllers to offer data subjects the right to opt out of the processing of their personal data for direct marketing purposes.

**Employee monitoring**

Employee monitoring is strictly regulated under Belgian law. Apart from the rules embedded in the Camera Surveillance Act of 21 March 2007, which provide that the use of CCTV requires a separate registration with the DPA, the monitoring of employees by means of surveillance cameras in particular is subject to the provisions of Collective Bargaining Agreement No. 68 of 16 June 1998. Pursuant to this Agreement, surveillance cameras are only allowed in the workplace for specific purposes:

1. the protection of health and safety;
2. the protection of the company’s assets;
3. control of the production process; and
4. control of the work performed by employees.

In the latter case, monitoring may only be on a temporary basis. Employees must also be adequately informed of the purposes and the timing of the monitoring.

With respect to monitoring of emails and internet use, Collective Bargaining Agreement No. 81 of 26 April 2002 imposes strict conditions. Monitoring cannot be carried out systematically and on an individual basis. A monitoring system of emails and internet use should be general and collective, which means that it may not enable the identification of individual employees. The employer is only allowed to proceed with the identification of the employees concerned if the collective monitoring has unveiled an issue that could bring damage to the company or threaten the company’s interests or the security of its IT infrastructure. If the issue only relates to a violation of the internal (internet) policies or the code of conduct, identification is only allowed after the employees have been informed of the fact that irregularities have been uncovered and that identification will take place if irregularities occur again in the future. In 2012, the DPA issued a specific recommendation...
on workplace cyber-surveillance. In this regard, the DPA advises employers to encourage employees to label their private emails as 'personal' or to save their personal emails in a folder marked as private. Furthermore, companies should appoint a neutral party to review a former or absent employee’s emails and assess whether certain emails are of a professional nature and should be communicated to the employer.

Finally, GPS monitoring in company cars is only allowed under Belgian law with respect to the use of the company car for professional reasons. Private use of the company car (i.e., journeys to and from the workplace and use during private time) cannot be monitored.

**Right to be forgotten**

In a judgment issued on 12 May 2016, the Belgian Supreme Court ruled that the right to be forgotten also applies to electronic archives of newspapers. The Supreme Court argued that the online publication of a case from over 20 years ago (a traffic accident reported in *Le Soir* in 1994), was likely to cause damage to the individual in the present. According to the Supreme Court, this would affect the individual’s right to privacy in a disproportionate manner, notwithstanding the interests of the newspaper and its freedom of expression (see Section VII).

The right to be forgotten, or the right to erasure (i.e., an individual’s right to have once public data about oneself removed from public access or to have private information erased) will also be buttressed by the GDPR. Pursuant to Article 17 of the GDPR, an individual has the right to demand that a data controller erase all personal data, without undue delay, on a number of occasions (e.g., no longer necessary for its purpose and unlawfully processed).

Although the right to be forgotten or to have data erased is not an absolute right and there are some limitations to it (e.g., freedom of expression and information, and reasons of public interest or public health), this right belongs to the individual. As such, a data controller cannot waive or opt out of compliance. If none of the exceptions of Article 17 apply, compliance with this right is mandatory. In making compliance mandatory, the GDPR will shift to the data controller the burden of proving that it falls under an exception of Article 17.

**IV INTERNATIONAL DATA TRANSFER**

Cross-border data transfers within the EEA or to countries that are considered to provide adequate data protection in accordance with EU and Belgian law are permitted. Transfers to other countries are only allowed if the transferor enters into a model data transfer agreement (based on the EU standard contractual clauses) with the recipient or if the transfer is subject to binding corporate rules (BCRs).

If an international data transfer is concluded under the EU standard contract clauses, a copy of these must be submitted to the DPA for information. The DPA will check their compliance with the standard contractual clauses and will subsequently inform the data controller whether the transfer is permitted. Data controllers need to wait for this confirmation from the DPA before initiating their international data transfer.

In the case of non-standard *ad hoc* data transfer agreements, the DPA will examine whether the data transfer agreement provides adequate safeguards for the international data transfer. If the DPA believes that the safeguards are adequate, the Ministry of Justice will, on verifying the entity’s compliance with the applicable procedural rules, approve the agreement by Royal Decree.
If a data controller gives ‘sufficient guarantees’ for adequate data protection by adopting BCRs, a copy of the BCRs also needs to be sent to the DPA for approval. Pursuant to the Protocol of 13 July 2011 between the DPA and the Ministry of Justice, if the DPA’s opinion is favourable, the Ministry of Justice will, on verifying that the process specified in the Protocol has been followed, approve the BCRs by Royal Decree.

Data transfers to the United States also used to be allowed if the recipient had committed to the Safe Harbor Principles. In its ruling of 6 October 2015, however, the CJEU concluded that the Safe Harbor regime is invalid and does not prevent national data protection authorities from assessing the adequacy of the protection granted by US recipients that are Safe Harbor-certified, and from prohibiting transfers to the United States (or imposing stricter conditions). This gave rise to negotiations between the EU and the United States regarding the legal framework for the data transfers. On 12 July 2016, the European Commission adopted the EU–US Privacy Shield, which meets the requirements as set by the CJEU (i.e., adequate protection of personal data and clear safeguard and transparency obligations).

After approximately a year of the EU–US Privacy Shield being in place, at the end of September 2017, officials from the US government, the European Commission and EU data protection authorities gathered in Washington to review it for the first time. They examined the administration and enforcement of the Privacy Shield, including commercial and national security-related matters, as well as broader US legal developments. The conclusion was that the Privacy Shield continues to ensure an adequate level of data protection, but that there is room for improvement. To achieve this, the European Commission has drawn up a list of recommendations on the functions of the Privacy Shield that need to be improved by the US authorities. The United States and the EU continue to collaborate and remain committed to ensuring the Privacy Shield functions as intended.

As an exemption to the above, transfers to countries not providing adequate protection are also allowed if the transfer:

- is made with the data subject’s consent;
- is necessary for the performance of a contract with, or in the interests of, the data subject;
- is necessary or legally required on important public interest grounds or for legal claims;
- is necessary to protect the vital interests of the data subject; or
- is made from a public register.

V COMPANY POLICIES AND PRACTICES

Although companies are not explicitly required under Belgian law to have online privacy policies and internal employee privacy policies, in practice they need to have such policies in place. This results from the obligation, under Belgian data protection law, for data controllers to inform data subjects of the processing of their personal data (including the types of data processed, the purposes of the processing, the recipients of the data, the retention term, information on any data transfers abroad, etc.). As a result, nearly all company websites contain the required information in the form of an online privacy policy.

Likewise, companies often have a separate internal privacy policy for their employees, informing the latter of the processing of their personal data for HR or other purposes. Such a policy sometimes also includes rules on email and internet use. Some companies include the privacy and data protection information in their work regulations. This is the document
that each company must have by law and that sets out the respective rights and obligations of workers and employers. The work regulations also provide workers with information about how the company or institution employing them works and how work is organised.

The appointment of a chief privacy officer is not very common in Belgium, except within large (and mostly multinational) corporations. Such corporations often also have regional privacy officers. In smaller companies, the appointment of a chief privacy officer is rare. However, given the increasing importance of privacy and data security, even smaller companies often have employees at management level in charge of data privacy compliance (often combined with other tasks).

In this respect, it should be noted that in Belgium, unlike some other European countries, the appointment of an independent data protection officer, who is responsible for compliance and acts as the go-to person for the authorities, is not required by law.

Although it is only considered best practice at present, the upcoming GDPR contains an obligation to conduct a data protection impact assessment (DPIA) for high-risk data processing activities. The DPA has taken the liberty of issuing recommendations on the DPIA requirement of the GDPR. In addition to the non-exhaustive list of processing activities as envisaged by the GDPR (i.e., any processing that entails a systematic and extensive evaluation of personal aspects that produce legal effects; any processing on a large scale of special categories of data; and any systematic monitoring of a publicly accessible area on a large scale), the DPA clarifies its position on what qualifies as high risk, when a DPIA must be conducted, what it should entail and when it should be notified of the results of a DPIA. The main takeaway of the DPA’s statement is that it should only be notified of processing activities where the residual risk (i.e., the risk after mitigating measures have been taken by the controller) remains high. Whether the DPA’s position will be supported at EU level remains to be seen, since the interpretation of DPIA methodologies is in principle an EU-level matter.

A substantial number of companies have conducted privacy audits in the past decade to get a clear view on their data flows and security measures. These audits have often resulted in the implementation of overall privacy compliance projects, including the review and update of IT infrastructure, the conclusion of data transfer agreements or adoption of BCRs and the review and update of existing data processing agreements with third parties.

In large organisations, it is considered best practice to have written information security plans. Although this is also not required by law, it proves very useful, as companies are required to present a list of existing security measures when they notify their data processing operations to the DPA. The DPA has also recommended that companies have appropriate information security policies to avoid or address data security incidents.

On 14 June 2017, the DPA published a recommendation on processing-activity record-keeping. As from the entry into force of the GDPR in 2018, organisations processing personal data within the EU must maintain records of their processing activities. Organisations with fewer than 250 employees are exempted from keeping such records, unless their processing activities:

- are likely to result in a risk to the rights and freedoms of data subjects (e.g., automated decision-making);
- are not occasional; or
- include sensitive data.
On the basis of the above-mentioned non-cumulative conditions, it may be expected that basically all organisations processing personal data will have to maintain records of their processing activities in practice, even if they employ fewer than 250 people.

In substance, these records should contain information on who processes personal data, what data is processed and why, where, how and for how long data is processed.

VI DISCOVERY AND DISCLOSURE

Pursuant to the Belgian Code of Criminal Procedure, the public prosecutors and the examining magistrates have the power to request the disclosure of personal data of users of electronic communications services (including telephone, email and internet) in the context of criminal investigations. Examining magistrates may also request technical cooperation of providers of electronic communications service providers and network operators in connection with wiretaps.

The personal and territorial scope of application of these powers is currently the subject of a heated debate before the Belgian Supreme Court and criminal courts. In 2009, Yahoo! was prosecuted for non-compliance with the provisions of the Code of Criminal Procedure, as it had refused to disclose certain personal data related to a Yahoo! account that had been used in connection with a drug-related criminal offence. In addition, last year, Skype was charged with non-compliance as a result of its alleged lack of technical cooperation in connection with a wiretap on the communication of one of its Belgian users (see also Section II). The discussion in both cases deals with two issues: first, can Yahoo!, Skype and similar service or software providers be considered as providers of electronic communications services under Belgian law; and second, does the duty of cooperation set forth in the Belgian Code of Criminal Procedure apply to foreign entities that have no physical presence (no offices, infrastructure, servers, etc.) in Belgium – and if so, can it be enforced against them by the Belgian courts?

A detailed discussion of both questions is beyond the scope of this chapter, but it is interesting to note that the Supreme Court has already issued two surprising decisions in the Yahoo! case that may have far-reaching consequences. In its first decision, the Court has extended the scope of the definition of providers of electronic communications services, so that it includes not only service providers that take care of the transmission of signals and data over the electronic communications networks, but also ‘anyone offering a service that allows its customers to obtain, receive or spread information via an electronic communications network’. This new definition seems problematic for multiple reasons. First, the Supreme Court disregards the very clear definition of ‘providers of electronic communications services’ set forth in the Act of 13 June 2005 on electronic communications. Second, its own definition is very vague and gives courts a great margin of appreciation, which goes against the principle of legal certainty (in particular in criminal matters). However, it can be expected that in the future, the duty to disclose personal data will apply not only to traditional internet access providers and telephone companies, but also to a wide variety of online software or service providers. Currently, the Belgian parliament is debating a draft proposal of the law that intends to extend the scope of application of the cooperation duty to all service providers meeting the definition offered by the Supreme Court.

The second decision of the Supreme Court in the Yahoo! case is even more important from an international perspective: the Court ruled that even though Yahoo! had no physical presence in Belgium, the provisions of the Code of Criminal Procedure applied to it, as the
'service' it offers can be used in Belgium via the internet. It also stated that the fact that the public prosecutor sent the request to disclose personal data directly to Yahoo! in the United States (without making use of the procedures set out in the applicable treaties regarding mutual legal assistance in criminal matters) did not make the request invalid or unenforceable.

This latter decision essentially implies that foreign entities offering an online service (or software) are subject to Belgian criminal law as soon as the software service can be used in Belgium, and that the Belgian public prosecutor has the power to enforce Belgian criminal law against such foreign entities without the intervention or assistance of the judicial authorities of the state of residence of these entities. Obviously, this position taken by the Supreme Court would also imply that foreign judicial authorities could enforce their national criminal law against service providers located in Belgium and do so without assistance from the Belgian courts.

Finally, on 1 December 2015, the Supreme Court put an end to the legal proceedings by rejecting the appeal, thereby confirming the Court of Appeal’s decision, which has caused important implications for the international system of mutual legal assistance in criminal matters.

Analogously, the Court of First Instance of Mechelen condemned Skype Communications SARL, a Luxembourg-based entity, for refusing to set up a wiretap in Mechelen in its ruling of 27 October 2016. The wiretap concerned was ordered by the Mechelen examining judge in the framework of an investigation into a Skype user. Again, the Belgian authorities ignored the European Convention on Mutual Assistance in Criminal Matters and imposed the wiretap order directly on Skype in Luxembourg. The Court of Mechelen applied a similar reasoning to that applied by the Supreme Court in the Yahoo! case and held that the alleged offence, namely the refusal to provide technical assistance, can be deemed to have occurred in the place where the information should have been received, regardless of where the operator was established.

Notably, the context of the Skype case is totally different from the situation in the Yahoo! case. While the Yahoo! case involved the mere refusal to disclose information to the Belgian authorities (Section 46 bis Section 1 of the Belgian Code of Criminal Procedure), the Skype case concerns the refusal to set up a wiretap (Article 88 bis Section 2 and Article 90 quater Section 2 of the Belgian Code of Criminal Procedure). The latter is undeniably a completely different type of measure, encompassing not only the provision of information, but also material acts by Skype and the necessary technical infrastructure to perform them, which Skype did not have in Belgium. Unsurprisingly, Skype appealed against this judgment before the Court of Appeal of Antwerp. The final judgment is expected before the end of 2017.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Belgian enforcement agency with responsibility for privacy and data protection is the DPA.

The DPA’s mission is, inter alia, to monitor compliance with the provisions of the Data Protection Act. To this end, the DPA has general power of investigation with respect to any type of processing of personal data and may file a criminal complaint with the public prosecutor. It may also institute a civil action before the president of the court of first instance. However, the DPA cannot impose any administrative penalties upon individuals or
Belgium

organisations. In response to complaints filed by individuals, it will try to reach a solution by mediating between the parties, but if no solution can be found, the parties will need to go to court to settle their dispute.

Whereas the DPA currently only has limited sanctioning powers, the Belgian Council of Ministers recently approved a draft law to reform the DPA in light of the forthcoming GDPR. The reformed DPA will be an independent administrative authority with legal personality and extensive investigative and sanctioning powers, composed of six different bodies: an executive committee, a general secretariat, a front-line service, a knowledge centre, an inspection service and a dispute chamber.

The executive committee, composed of the leaders of the five other bodies, will be responsible for the adoption of the DPA's general policies and strategic plan.

A general secretariat will be established for the reception and processing of complaints and to inform citizens about their data protection rights.

The inspection service will function as the investigating body of the DPA, with a wide array of investigative powers (e.g., interrogation of individuals).

The front-line service will have a singular role in providing guidance (e.g., with regard to adequate data protection techniques under the GDPR) and supervising data controllers and processors and their compliance with data protection legislation.

Led by six experts in the field, the knowledge centre will provide public decision-makers with the necessary expertise to understand the technologies likely to impact on the processing of personal data.

The dispute chamber, composed of a president and six judges, will be able to impose sanctions of up to €20 million or up to 4 per cent of the total worldwide annual turnover of the infringing company.

As well as the above-mentioned bodies being established under the auspices of the reformed DPA, an independent think tank will be set up to reflect society as a whole, both participants in the creation of the digital world and those affected by it, and to provide the executive committee with a broad vision and guidance as it negotiates current and future data protection challenges.

Another novelty of the draft law is that, along with natural persons, legal persons, associations or institutions will also be able to lodge a complaint of an alleged data protection infringement.

In spite of the expansion of the DPAs powers, the government unfortunately decided not to increase its budget. In other words, the DPA will have to perform more tasks but with the same resources. Given the fact that, at present, the DPA only rarely conducts raids and investigations because of a lack of resources, it remains to be seen whether in future the DPA will be little more than a toothless tiger, new powers notwithstanding.

Recent investigations by the DPA concern the data processing practices of Belgium’s largest telecom service providers: Telenet and Proximus.

The DPA investigated Telenet’s direct marketing practices and examined whether Telenet was collecting its customers’ prior and specific opt-in consent. In contrast to its regime for new customers, Telenet applied an opt-out regime for existing customers. According to the DPA, such an opt-out approach is unlawful as it does not adhere to the consent requirements laid down in the Data Protection Act (i.e., prior, free, specific, unambiguous and informed consent). Furthermore, the DPA raised concerns about whether Telenet customers had been
informed of the new processing activities in a clear and understandable manner. At present, the DPA is further investigating the matter and has engaged in discussions with Telenet to address the concerns raised.

Proximus, on the other hand, is planning to offer a tailored advertising service based on anonymised and aggregated (location) data of its end users. After investigation, the DPA found that the location data and otherwise encrypted data could still be connected to the data of an identified customer and therefore concluded that the Proximus anonymisation process was inadequate. Further to the DPA’s findings, Proximus adapted its service to ensure adequate anonymisation of its customers’ location data.

ii Recent enforcement cases
The most important recent enforcement case undertaken by the DPA is the one initiated against Facebook in June 2015. In May 2016, the Court of Appeal of Brussels overruled the interlocutory judgment of the President of the Court of First Instance imposing interim measures on Facebook, partially on jurisdictional grounds and partially because of a lack of urgency. For now, the DPA awaits the decision of the Court of First Instance of Brussels on the merits of the case and, particularly, the Court’s answer to the question of who has jurisdiction over Facebook and is competent to judge the alleged privacy infringements. This decision on the substance of the DPAs claim is expected to be delivered later this year. The DPA has already been investigating the possibility of bringing the case before the Belgian Supreme Court if its claim against Facebook is rejected (see also Section II).

In a non-binding opinion, an advocate general of the Court of Justice of the European Union has recently stated that Facebook should indeed adhere to the national privacy rules of EU Member States if it collects and processes data from users in those Member States and has a physical establishment (e.g., a sales office) on their territory. Hence, the advocate general opposes Facebook’s argument that it should comply only with Ireland’s privacy legislation, the country where it has its European headquarters.

In addition to the Facebook case, the most important enforcement cases before the Belgian courts are the Yahoo! and Skype cases, discussed in Sections II and VI.

With respect to cases handled by the DPA, no information about individual complaints has been made publicly available. According to the DPA’s Annual Report of 2016, the DPA processed 4,491 requests or complaints (an increase of 299 compared with 2015), including requests for information, mediation and control. The majority of information requests related to the use of CCTV, data subjects’ rights, the right to one's image, data processing registrations and contractual clauses.

iii Private litigation
Private plaintiffs may seek judicial redress before the civil courts on the basis of the general legal provisions related to tort or, in some cases, contractual liability. In addition, they may file a criminal complaint against the party that committed the privacy breach. Financial compensation is possible, to the extent that the plaintiff is able to prove the existence of damages as well as the causal link between the damage and the privacy breach. Under Belgian law, there is no system of punitive damages.

Class actions were traditionally not possible under Belgian law until 1 September 2014, when a new Act on Class Actions entered into force. So far, there are no known cases of class action lawsuits filed in connection with data privacy.
In April 2016, the Supreme Court ruled in favour of the right to be forgotten. The case concerned the online disclosure of an archived database of a famous Belgian newspaper, which would result in the publication of the full name of a driver who was involved in a car accident in 1994 in which two people died. Both the Court of Appeal and the Supreme Court considered the right to be forgotten essential in this case and ruled in favour of a limitation of the right of freedom of expression (see also Section III.iv).

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Organisations based or operating outside Belgium may be subject to the Belgian data protection regime to the extent that they process personal data in Belgium. Physical presence in Belgium (either through a local legal entity or branch office, with or without employees, or through the use of servers or other infrastructure located on Belgian territory) will trigger the jurisdiction of Belgian privacy and data protection law even if the personal data that is processed in Belgium relates to foreign individuals. Foreign companies using cloud computing services for the processing of their personal client or employee data may therefore be subject to Belgian law (with respect to such processing) if the data is stored on Belgian servers.

In principle, the mere provision of online services to persons in Belgium, without actual physical presence, will not trigger Belgian jurisdiction. However, as discussed under Section VI, according to a recent Supreme Court decision, the Belgian judicial authorities would have jurisdiction over foreign entities providing online services or software to users in Belgium, even if they are not present in Belgium. This is certainly an issue to follow up, as it may have an important impact on the territorial scope of application of Belgian law, especially in light of the entry into force of the GDPR on 25 May 2018.

It should be noted that the GDPR will even apply to data controllers having no presence at all (establishment, assets, legal representative, etc.) in the EU but who process EU citizens’ personal data in connection with goods or services offered to those EU citizens; or who monitor the behaviour of individuals within the EU.

IX CYBERSECURITY AND DATA BREACHES

As a member of the Council of Europe, Belgium entered into the Council’s Convention on Cybercrime of 23 November 2001. Belgium implemented the Convention’s requirements through an amendment of the Act of 28 November 2000 on cybercrime, which introduced cybercrime into the Belgian Criminal Code. With the Act of 15 May 2006, Belgium also implemented the requirements of the Additional Protocol to the Convention on Cybercrime of 28 January 2003 concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

As previously mentioned, the CCB will:

a monitor Belgium’s cybersecurity;
b manage cybersecurity incidents;
c oversee various cybersecurity projects;
d formulate legislative proposals relating to cybersecurity; and
e issue standards and guidelines for securing public sector IT systems.

Since becoming operational at the end of 2015, the CCB has carried out several awareness campaigns; for instance, in the context of the Petya ransomware cyberattacks and the ‘CEO
fraud’ (a large-scale scam where cybercriminals contact a company as the alleged CEO of another big company with a request to make an important payment into the first company’s bank account).

Furthermore, the management of CERT, which has been in the hands of Belnet since 2009, was transferred to the CCB in December 2016. The transfer of all CERT activities is part of the continuing coordination of Belgian cybersecurity and is aimed at assisting companies and organisations in the event of cyber-incidents by providing advice both about finding solutions when such incidents arise and about preventing incidents occurring.

Additionally, the Belgian Cyber Security Coalition, which is a partnership between parties from the academic world, public authorities and the private sector, was established in October 2014. Currently, more than 50 key participants from across the three sectors are active members. These include large financial institutions, universities, consultancy companies, professional organisations and government bodies. The main goals of the Coalition are to raise awareness about cybersecurity, exchange know-how, take collective actions in the fight against cybercrime and support governmental and sectoral bodies in setting policies and determining ways to implement these policies.

With respect to data breach notifications, Article 114/1, Section 2 of the Electronic Communications Act requires companies in the telecommunications sector to notify immediately (within 24 hours) personal data breaches to the DPA, which must transmit a copy of the notification to the Belgian Institute for Postal Services and Telecommunications. If there is a breach of personal data or the privacy of individuals, the company must also notify the data subjects affected by the breach.

The Data Protection Act does not, however, provide for a general data breach notification obligation, as is provided for in the GDPR. In 2013, the DPA was confronted by a series of data security incidents of which it only became aware after those incidents were published in the media. Unable to change the legislation itself (which, of course, would require legislative intervention), the DPA issued a recommendation upon its own initiative stating that it considered data breach notifications to be an inherent part of the general security obligations incumbent on any data controller.

More specifically, the DPA's recommendation stressed the importance of conducting risk assessments and implementing appropriate security measures (including security policies), and noted that incident management policies should specify that ‘in the event of public incidents the competent authorities [i.e., the DPA] must be informed within 48 hours of the causes and damage’. Although the concept of a ‘public incident’ is not explained in greater detail, one may assume that this term refers to an incident in which data are lost, destroyed, altered or disclosed in a way that is likely to become known to the public or the DPA via, for example, the media, the internet or complaints from individuals. It is to be expected that this recommendation by the DPA will be transposed into a legal obligation as soon as the GDPR enters into force.

In relation to data security, the International Chamber of Commerce in Belgium and the Federation of Enterprises in Belgium, together with the B-CCentre, have taken the initiative to create the Belgian Cyber Security Guide in cooperation with Ernst & Young and Microsoft. The Guide is aimed at helping companies protect themselves against cybercriminality and data breaches. To that effect, it has listed 10 key security principles and 10 ‘must do’ actions, including user education, protecting and restricting access to
information, keeping IT systems up to date, using safe passwords, enforcing safe-surfing rules, applying a layered approach to viruses and other malware, and making and checking backup copies of business data and information.

X OUTLOOK

With regard to the entry into force of the GDPR next year, the overall focus of the DPA will obviously be on preparing companies, data controllers and data processors for this new EU data protection framework. To this end, the DPA has already launched a new section dedicated to the GDPR on its website and a 13-step plan for companies involved in data collection or processing, or both, to help them comply with the forthcoming new rules of the GDPR.

Apart from the strengthening of the investigative and sanctioning powers of the DPA (see Section VII), we do not expect the GDPR to result in any major changes to the Belgian situation in practice. Belgium's legislation and the interpretation given to it by the DPA have traditionally been in line with EU law and the positions of the European Commission and the Article 29 Working Party.

As mentioned above (see Section VII), the investigative and sanctioning powers of the DPA will be significantly expanded under the GDPR. Unfortunately, the government decided not to increase its budget. As a result, the DPA is expected to have only very limited resources to support the use of its new powers and launch data protection investigations or conduct raids. We believe that the prospect of prosecutions being initiated by the DPA will remain rather unlikely given these budgetary constraints. Nevertheless, in the event of a complaint being lodged with the DPA or of a data breach incident, it will have broader competence to examine the complaint and to impose higher sanctions on the alleged violator.

In its assessment of alleged data protection violations, the DPA will definitely check whether sufficient efforts have been made to meet the requirements laid down in the GDPR.
I OVERVIEW

Brazil is one of the countries with the highest number of internet users in the world. The fact that the use of internet and digital technologies has boosted the collection, storage and use of data in Brazil underlines the importance of protecting users’ privacy and their personal data, as well as the urgent need to regulate the treatment and use of personal data in Brazil.

The increased use of the internet and mobile devices on one side and developments in the area of digital technology on the other have proved challenging in relation to the collection and use of information and personal data. With much more user-related data (including personal information and data, and consumer behaviour and health data) being generated, protection of privacy and regulation of the collection, storage, use and sharing of personal data has become an important issue in Brazil.

Although the use of personal data is regulated in most Western countries, there is a lack of regulation in this field in Brazil as privacy and data protection are treated as distinct concepts, although they both derive from the right to privacy, which is enshrined as a constitutional principle. While privacy is regulated in the Brazilian Civil Code (Article 21), data protection demands specific rules. In this regard, Law No. 12.965 (Brazil’s Civil Rights Framework for the Internet) regulates aspects of data privacy within the framework of the internet; however, it only applies to the collection, storage and use of data in the context of the internet. Outwith the context of the internet, there are no statutes regulating data protection in general, although some sector-specific laws regulate the protection of personal data and there are also bills currently under consideration in Congress that aim to regulate the protection and treatment of personal data in general in the Brazilian territory. Cybersecurity, however, is regulated in the criminal sphere in Brazil, as outlined in Section IX.
II THE YEAR IN REVIEW

Brazil has not seen further regulation in the field of data protection since the issuance of Decree No. 8.771/2016 by former President Dilma Rousseff. Currently, there are bills to regulate data protection in general under consideration by Congress; however, it is not possible to say when Congress will pass these into law.

In the field of case law, a Brazilian federal public prosecutor from the state of Piauí filed a lawsuit against Google requesting the suspension of the content scanning of users’ Gmail accounts, throughout the Brazilian territory, until prior and express consent is obtained from users. On 23 June 2017, the second-instance federal court judge issued a decision denying the preliminary order request by the federal public prosecutor. The federal judge stated that the case did not meet the legal requirements for granting such an order. We await with interest further developments in this case regarding content scanning of users’ emails and online behavioural advertising.

The State Court of Justice of São Paulo issued a decision against technology company Apple in relation to illegal access of an iCloud cloud storage account by a third party. The plaintiff filed a lawsuit against Apple to request the internet protocol (IP) address and related data for the user who accessed the plaintiff’s iCloud account and erased all related content from the account, and also to request the recovery of the files that had been stored in the account. The São Paulo State Court ordered Apple to provide the IP address and related data under penalty of a fine of approximately US$1,000 per day; however, since the files were erased by the hacker, as demonstrated by the plaintiff, and companies cannot store users' files without previous and express authorisation, the court stated that Apple could not comply with the plaintiff’s request.

It seems that data protection regulation in the context of the internet and subsequent related decisions by Brazilian courts have ensured a safe path for companies to develop their business in Brazil. We expect the anticipated general data protection law, currently under consideration by Congress, may define the rights of individuals and clarify the law on the collection, storage, treatment, use and sharing of data in Brazil by Brazilian and foreign companies.

III REGULATORY FRAMEWORK

In Brazil, the right to privacy is protected by the Constitution of the Federative Republic (the Constitution), in which it is enshrined as a constitutional principle. In addition, the Brazilian Civil Code regulates the right to privacy (which applies generally for individuals) but does not regulate data protection.

Currently, there is no statute in Brazil to regulate data protection in general. Notwithstanding this, some sector-specific laws provide rules related to the protection of personal data in narrow economic sectors (e.g., banking and telecommunications) and in certain professional (e.g., law, medicine and accounting) and public fields. Furthermore, Brazil’s Civil Rights Framework for the Internet (Law No. 12.965) regulates data protection

---

3 Decree No. 8.771/2016 regulating Law No. 12.965 of 23 April 2014 was one of President Dilma Rousseff’s final acts in post and was issued hours before her removal as president.
4 Article 5, X.
6 See the Brazilian Information Access Act.
in relation to the internet and is applicable to the collection, storage and use of data on the world wide web. Law No. 12.965, a unique internet-related statute that has influenced other legislation around the world, establishes the principles, guarantees, rights and obligations for the use of the internet in Brazil. It focuses on the protection of rights in the context of the internet and regulates aspects of data privacy within the legal framework for the internet.

It is important to reiterate that Law No. 12.965 only regulates internet-related data privacy and does not extend to the collection, storing and processing of personal data outwith the context of the internet.

Law No. 12.965 implements internet-related civil rights in Brazil and imposes obligations on internet service providers and internet users in the Brazilian territory. Among other rules, it establishes principles for internet use in Brazil, namely:

a. freedom of speech, communication and expression, pursuant to the Constitution;
b. the protection of privacy;
c. the protection of personal data in accordance with the law;
d. the preservation and guarantee of net neutrality according to the regulations;
e. the preservation of the stability, security and functionality of the network by means of technical practices compatible with international standards, and through incentives for the use of best practices;
f. the liability of agents, according to their activities, in line with the law; and
g. the preservation of the participatory nature of the internet.

Particular attention should be paid to the fact that the above-mentioned principles defined by Law No. 12.965 do not exclude other relevant provisions set out by the national legal system, or by those established under international treaties signed by Brazil.

Further, Law No. 12.965 guarantees users the following rights:

a. the right to the non-violation and secrecy of their communications, except when the subject of a court order, pursuant to specific clauses determined by law, for the purpose of a criminal investigation or in the course of a criminal lawsuit;
b. the right to have clear and comprehensive information included in contracts with providers that expresses the regime for the protection of personal data, connection logs and internet service access logs, as well as information on the providers’ adopted practices for network management that might affect the quality of service offered; and
c. the right to the non-disclosure or use of connection logs and internet service access logs, except with express consent or when the subject of a court order.

Under Law No. 12.965, the keeping of records and the provision of connection and access to the internet, must comply with the preservation of the privacy, private life, honour and image of parties. Breach of this rule shall subject the provider to civil, criminal and administrative sanctions provided by law.

Furthermore, under Law No. 12.965, providers of internet applications may only be liable for damages arising out of content that is generated by third parties if, after receiving a specific court order regarding the content, they do not take any steps – within the framework of their services and within the period provided – to make the illegal content unavailable.

Approval of a statute for the regulation of data protection is quite important for the further development of data protection in Brazil, since Law No. 12.965 applies only to internet-related issues. As such, in cases of intranet issues or other situations not connected with the use of the broader internet in Brazil, Law No. 12.965 does not apply, so individuals,
companies and organisations seeking relief in court must base their case on constitutional principles and rules. Furthermore, it is, in fact, possible to apply constitutional and general civil rules to enforce the right of privacy, despite this absence of general rules regarding personal data.

In contrast, the Brazilian Copyright Law has a specific provision on data protection – although it only protects the titleholder of the collected data. These general provisions, however, do not reflect the necessary grounds for ensuring clear and transparent rules relating to personal data protection through networks.

In the criminal sphere, the Brazilian legal system does not have specific legislation covering violations of protected data, so the penalties applied to offenders who disclose secret data or data that violate the intimacy, private life, honour and image of a person are established sparsely and in various legal provisions, including the following examples. With regard to the protection of children and adolescents, Articles 17, 18, 143 and 247 of Law No. 8.069/90 contain rules to protect the image and reputation of children and adolescents by punishing anyone who exposes them in a negative or injurious manner. The protection of banking and tax secrecy is established by Article 5, X of the Constitution, with some exceptions set out in Complementary Law No. 105/01. Specifically regarding taxation, Article 198 of the National Tax Code establishes sanctions for violations of fiscal secrecy, as do Articles 154 and 325 of the Penal Code, which cover unauthorised revelation of secrets in general.

---

7 Law No. 9610 of 19 February 1998 on Copyright and Neighbouring Rights:

87. The owner of the economic rights in a database shall enjoy the exclusive right to authorise or prohibit the following in relation to the form of expression of the structure of that database:

I. complete or partial reproduction by any means or process;

II. translation, adaptation, rearrangement and any other modification;

III. distribution of the original or copies of the database, or communication of the database to the public;

IV. reproduction, distribution or communication to the public of the results of the operations referred to in item II of this Article.


9 Law No. 5.172/66 on the National Tax System and Establishing General Rules of Tax Law Applicable to the Union, States and Municipalities: www.planalto.gov.br/ccivil_03/leis/L5172Compilado.htm (last accessed on 26 August 2016).

Art. 198. Without prejudice to the provisions of criminal legislation, the disclosure by the Tax Administration or its civil servants of information obtained by reason of their authority about the economic or financial situation of taxpayers or third parties and about the nature and the state of their business affairs or activities is forbidden.


Art. 154. To reveal to someone, without just cause, a secret one learns by reason of one's function, position, trade or profession and whose revelation can produce damage to another person:

Penalty – detention of three months to one year, or a fine.

Art. 325. To reveal a fact one learns by reason of one's position and that must remain secret, or to facilitate the revelation thereof:

Penalty – detention of six months to two years, or a fine, if the fact does not constitute a more serious crime.
The secrecy of telephonic, telegraphic and computerised communications is covered by Law 9.296/96, which regulates Article 5, XII of the Constitution, according to which ‘the secrecy of correspondence, telegraphic communications, data transmission and telephonic communications is inviolable, except, in the last case, by court order, in the situations and in the form established by law for purposes of criminal investigation or to obtain evidence in a criminal proceeding’.

Law 9.296/96, in Article 10, defines as criminal the interception of telephone or computer communications or the breach of judicial secrecy without a court order or with objectives not authorised by law. Violation is punishable by two to four years in prison and a fine.

IV INTERNATIONAL DATA TRANSFER

Brazil currently has no regulation on international data transfer, although there are bills under consideration by the Brazilian Congress to regulate the processing of personal data, including international data transfers.

Nevertheless, Law No. 12.965 states that in any operation for the collection, storage, retention and treatment of personal data by internet application providers where at least one of these acts takes place in the Brazilian territory, Brazilian law must be mandatorily respected regarding the protection of personal data, even if the activities are carried out by a legal entity based abroad, provided that it offers services to the Brazilian public, or at least one member of the same economic group is established in Brazil. Thus, whether or not a foreign company intends to collect data in Brazil for transfer to other countries, Brazil’s Law No. 12.965 applies to the collection, storage, retention and treatment of the personal data collected.

V COMPANY POLICIES AND PRACTICES

Law No. 12.965 regulates the collection, storage and treatment of personal data in the context of the internet. According to this Law, internet providers must obtain the previous authorisation of individuals to collect, store and treat their data, and must delete any collected, stored and treated data if so required by the individual.

To comply with the requirements of Law No. 12.965, it is duly recommended that any internet provider to adopt and make available for internet users online privacy policies and the terms of use of websites or platforms.

VI DISCOVERY AND DISCLOSURE

As previously mentioned, protection of privacy and intimacy in general is set out in Article 5, X of the Constitution. The right of privacy and intimacy is enshrined in the list of fundamental rights or, according to Ingo Sarlet, first-generation rights, so that the right of privacy and intimacy can only be relaxed to optimise or safeguard another fundamental right.

Again according to that legal scholar, the relaxation of guarantees can only occur when they collide with other guarantees, and only to the extent indicated by weighing up the

---

11 Law No. 9.296/96 Regulating Numeral XII, Final Part, of Article 5 of the Constitution: www.planalto.gov.br/ccivil_03/leis/L9296.htm (last accessed on 26 August 2016).
different rights or by applying the principle of proportionality. Therefore, in the ambit of criminal investigations, unless a specific law exists authorising it, the breach of privacy is subject to judicial reservation, meaning that the investigatory authority (the police or public prosecution service) must obtain a court order to override the secrecy of private information (inter alia, bank and tax data, personal information, telephone communications, written communications, data exchange).

With respect to requests for information by investigatory bodies in the international arena, these will be subject to the existence of a mutual legal assistance treaty (MLAT) between Brazil and the other country. If no treaty for international cooperation in criminal matters exists, a request for private information protected by secrecy must be formulated by the foreign authority by means of a letter rogatory, addressed to the Superior Tribunal of Justice (STJ) (the highest court for non-constitutional matters). Only after this court grants exequatur can the request be sent to a local judicial authority with competence to order compliance with the request from the foreign authority.

The letter rogatory route is much slower than when an MLAT exists, for example, as happens between Brazil and the United States. As a rule, under MLATs, requests are made through a central authority designated by each country, thus obviating the need for a decision by the STJ in Brazil.

For example, in the case of a request for cooperation to obtain evidence in a criminal investigation where this is subject to the judicial reservation clause, the Brazilian Central Authority will send the request to the Federal Prosecution Service, which has competence to apply for court orders. Since judgment by the STJ is not necessary, direct requests for assistance (via MLATs) are faster and more efficient.

VII PUBLIC AND PRIVATE ENFORCEMENT

Brazil does not have a data protection authority yet. However, the consumer protection and defence authorities (PROCONs), which are local official bodies created both by Brazilian states and municipalities and by the federal district, are empowered to defend and protect the rights and interests of consumers. Thus, as PROCONs are currently in charge of the protection of consumers, they can prosecute and impose penalties on companies within their jurisdictions for consumer data protection and privacy-related offences.

Besides the PROCONs, the Brazilian Public Prosecutor’s Office may bring prosecutions before the courts, and its power encompasses not only consumer rights, but also all criminal- and internet-related issues. Moreover, individuals and companies may also enforce their own rights before the courts.

15 The judgment exercised by the STJ upon receiving a letter rogatory is restricted to verification of whether the request formulated by the foreign state satisfies the necessary formalities, without examining the merit of the question. If the formal aspects are satisfied, there is no violation of human rights and the statutory limitation period has not lapsed, the STJ will issue exequatur and send the request for cooperation to the competent authority (usually a federal court).
In internet-related matters, infringement of the data protection rules set out in Law No. 12.965 may result in the following sanctions, applied individually or cumulatively: (1) a warning establishing a deadline for the adoption of corrective measures; (2) a fine of up to 10 per cent of the gross income of the economic group in Brazil in the most recent fiscal year; (3) a temporary suspension of company activities related to the collection, storage, treatment and use of personal data; or (4) a prohibition on executing the company activities related to the collection, storage, treatment and use of personal data.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Because of considerations of space, infrastructure and convenience, companies are increasingly allowing their employees to work from home on some days of the week. These employees typically use their own mobile devices for work purposes, thus facilitating mobility and reducing company costs.

However, this ‘bring your own device’ arrangement potentially generates a serious problem: how can a company, if it is, for example, performing an internal audit as part of its compliance policy, have access to the data stored in the personal devices employees use for work? One solution to this problem can be the adoption of internal rules stipulating that all files and documents related to business activity be stored in a data cloud or filed on a shared company network.

However, another question arises: what can the company do to check whether an employee is storing work-related files or documents in a personal device rather than a shared company file?

In this case, as a rule unauthorised access to a mobile device is configured as a violation of information belonging to another party, defined as a crime in Article 154-A of the Brazilian Penal Code, so that a company policy requiring employees to allow access to their mobile devices would be illegal.

However, in the Brazilian legal system (other than for environmental crimes), only individuals can be held criminally liable, not companies. Therefore, in cases of unauthorised invasion of an electronic device, the crime will be imputed to the person within the company who carried out the invasion, along with the person who ordered this illegal action.

IX CYBERSECURITY AND DATA BREACHES

Since criminal law is the strongest expression of governmental power over individual freedom, the rational justification of the punitive system requires that the suppressive power of the government only be used when absolutely necessary, when other branches of law are not sufficient or able to protect rights. This is known as the principle of minimum intervention.


17 Penal Code, Article 154-A:

Art. 154-A: To invade another’s informatics device, connected or not to a network of computers, by undue violation of a security mechanism and with the purpose of obtaining, adulterating or destroying data without the express or tacit authorisation of the owner of the device, or to install security threats to obtain illicit advantage:

Penalty – detention of three months to one year, and a fine.
It is not difficult, especially in the Brazilian legal system, to observe the enactment of ‘emergency’ criminal laws. These are laws that are approved by legislators hastily in response to the media repercussion of a particular event or situation to satisfy the social clamour for ‘justice’. Often, these laws create new crimes or enhance penalties for existing ones that are unnecessary to protect the public interest, or that turn out to have unexpected negative consequences, flying in the face of the aforementioned principle, although this is by no means always the case, since the law must be agile to cover new technological developments.

In this respect, and specifically related to the privacy of digital data, mention can be made of Law 12.737/12, which introduced Article 154-A to the Penal Code. It is popularly called the Carolina Dieckmann Law, referring to the famous Brazilian actress who in 2012 had her intimate photos posted online after files from her digital camera were copied by a repair shop technician.

In defining a new type of crime, Brazilian lawmakers were faced with a question not specifically covered by criminal law, namely the invasion of electronic devices to obtain, adulterate or destroy data or information without the express or tacit authorisation of the owner, or to install security threats to obtain illicit advantage.

Therefore, the natural problem that arises is to what extent intervention by the criminal law is necessary. This requires facing the following questions:

a. If the type of crime did not exist, would the criminal law be able to protect the public against injury resulting from the conduct newly typified;

b. Is the state power, in its strongest expression, necessary, or would civil law and other branches of law suffice to redress the damage caused?

On the first question, although it can be said that Articles 158 and 171 of the Penal Code, covering extortion and larceny by fraud, are sufficient alone to punish installation of security threats in electronic devices, these crimes are limited to situations where the offender obtains an illicit advantage, while the new type of crime goes further by also covering mere invasion of privacy.

In turn, on the second question – obtaining, altering or destroying data – a parallel can be drawn with the violation of sensitive personal data (in corporate or personal systems) by companies, which not infrequently exchange or sell data and information about their customers to other companies.

In both cases, it can be argued that the damage caused can be satisfactorily redressed and the conduct suppressed, by civil law, through suits for compensation, independent of criminal liability of the offender.

---

19 Penal Code, Article 154-A.
20 Penal Code:

*Art. 158.* To restrain someone, by violence or grave threat, with the intent to obtain for oneself or another an undue economic advantage, or to tolerate doing or refraining from doing something:

*Penalty – imprisonment from four to ten years, and a fine.*

*Art. 171.* To obtain, for oneself or another, an illicit advantage, causing harm to another, by inducing or maintaining an error, through artifice, ruse or any other fraudulent means:

*Penalty – imprisonment of one to five years, and a fine of 500,000 reais to 10 million reais [in the Brazilian currency units at the time of enactment].*
In light of all the foregoing, we believe that privacy and intimacy are sufficiently protected in the Brazilian legal system. Nevertheless, as is typical of delinquency in general, those constitutional guarantees will always be targets of increasingly elaborate attacks, so the interpreters of the law must act diligently to frame the offending conduct within the existing legal rules and principles.

X OUTLOOK

As discussed above, privacy and intimacy are sufficiently protected in the civil and criminal spheres in Brazil. However, data protection is only regulated in the context of the internet by Law 12.965. In relation to this, two important bills (No. 4.060/2012 and No. 5.276/2016) under consideration by Congress aim to regulate data protection outside the context of the internet and we look forward to seeing whether Congress will pass these bills and introduce regulation of these rights in Brazil.
Chapter 8

CANADA

Shaun Brown1

I OVERVIEW

Privacy in Canada is regulated through a mix of constitutional, statutory and common law. The most fundamental protection is provided by Section 8 of the Charter of Rights and Freedoms, which states that ‘everyone has the right to be secure against unreasonable search or seizure’. This ensures a reasonable expectation of privacy for citizens in relation to the state.

There are also laws that establish when and how public sector bodies at the federal, provincial or territorial and municipal levels can collect, use and disclose personal information about citizens.

Beginning with Quebec in 1994, the private sector throughout Canada is now regulated by privacy legislation that applies generally to the collection, use and disclosure of personal information by all parts of the private sector. In addition, organisations in both the public and private sectors are increasingly required to defend privacy-related litigation based on statutory and common law torts.

This chapter focuses on the aspects of Canadian privacy law that apply to private sector organisations.

II THE YEAR IN REVIEW

The federal government delayed the private right of action under Canada’s anti-spam legislation (CASL),2 which was set to come into effect on 1 July 2017. The private right of action would allow individuals affected by violations of the law to sue for actual and statutory damages. The government cited concerns raised by businesses, charities and the not-for-profit sectors, and asked a parliamentary committee to review the legislation at the same time as it announced the delay.3

The federal government also published on 2 September 2017 draft regulations4 that provide further detail regarding the pending privacy breach notification requirements under

---

1 Shaun Brown is a partner at nNovation LLP.
2 An act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (SC 2010, c 23), s 47.
4 www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/pdf/g1-15135.pdf.
the federal Personal Information Protection and Electronic Documents Act (PIPEDA). A coming-into-force date for the data breach reporting requirements was not available at the time of writing.

The Federal Court of Canada affirmed that PIPEDA applies to organisations that collect, use and disclose personal information about Canadians in the course of commercial activity, even where those organisations have no physical presence in Canada. Further, the Supreme Court of Canada created a new form of implied consent under PIPEDA, finding that a debtor who defaulted on a loan had given implied consent to the debtor’s bank to disclose a mortgage statement to the lender so that it could enforce a judgment through the sale of the debtor’s home.

III REGULATORY FRAMEWORK

i Overview of privacy and data protection legislation and standards

Private sector organisations are subject to privacy legislation that applies generally to the collection, use and disclosure of personal information in the course of commercial activities throughout Canada. Given that there is shared jurisdiction for the regulation of privacy between the federal and provincial or territorial governments, organisations must be aware of the various laws that exist at those levels.

The federal PIPEDA, which began to come into force on 1 January 2001, applies to organisations that are federally regulated, including telecommunications service providers, railways, banks and airlines. It also applies to provincially and territorially regulated organisations in provinces and territories that have not passed their own private sector privacy legislation deemed to be ‘substantially similar’ to PIPEDA. Only three provinces currently have broad-based private sector privacy legislation in force: Alberta, British Columbia and Quebec.

Although there are some differences between these laws, they are generally similar in the most fundamental ways. Most importantly, fair information practice principles form the basis for these laws. In fact, PIPEDA incorporates into the text of the law the Canadian Standards Association Model Code for the Protection of Personal Information (CSA Model

---

5 SC 2000, c 5.
8 Alberta: Personal Information Protection Act, SA 2003, c P-6.5; British Columbia: Personal Information Protection Act, SBC 2003, c 63; Quebec: An Act respecting the Protection of Personal Information in the Private Sector, RSQ, c P-39.1. PIPEDA also does not apply to the collection, use and disclosure of personal health information by personal health information custodians that are subject to the New Brunswick Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05, the Newfoundland and Labrador Personal Health Information Act, SNL 2008, c P-7.01 or the Ontario Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A. Manitoba has passed private sector privacy legislation – the Personal Information Protection and Identity Theft Prevention Act, CCSM c P33.7 – that is generally similar to the laws in Alberta and British Columbia; however, it has neither been proclaimed in force nor deemed substantially similar to PIPEDA.
The CSA Model Code, which was developed through a collaborative effort involving industry, government and consumer groups and adopted in 1996, establishes the following 10 principles:

A accountability;
B identifying purposes;
C consent;
D limiting collection;
E limiting use, disclosure and retention;
F accuracy;
G safeguards;
H openness;
I individual access; and
J challenging compliance.

**ii Definition of personal information**

The most important concept under privacy legislation is ‘personal information’. Personal information is defined broadly as ‘any information about an identifiable individual’. The Supreme Court of Canada has held that this definition must be given a broad and expansive interpretation, and is much broader than the concept of ‘personally identifiable information’ that is referenced in some other jurisdictions.

Thus, personal information includes such things as a person’s name, race, ethnic origin, religion, marital status, educational level, email addresses and messages, internet protocol (IP) address, age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint, income, purchases, spending habits, banking information, credit or debit card data, loan or credit reports, tax returns, social insurance number or other identification numbers.

Information does not need to be recorded for it to be personal. For example, information could be in the form of an oral conversation, or real-time video that is not recorded.

One of the more contentious issues under Canadian law is when information is about a person who is ‘identifiable’. The Federal Court of Canada has held as follows: ‘information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information’.

The Privacy Commissioner of Canada (Commissioner), who is responsible for oversight of PIPEDA, has taken an expansive approach to this question in the past. For example, in one investigation involving the use of deep packet inspection technologies by an internet service provider (ISP), the Commissioner held that the IP addresses collected by the ISP were personal information even though they were not linked to individuals, because the ISP had the ability to make such a link.

Perhaps even more extreme is the Commissioner’s approach to online behavioural advertising (OBA). The Commissioner has taken the position that much of the information

---

12. *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, Paragraph 34.
used to track and target individuals with interest-based adverts online – including such things as IP addresses, browser settings, internet behaviour – is personal information even where individuals are not personally identified. The Commissioner explains as follows:

In the context of OBA, given the fact that the purpose behind collecting information is to create profiles of individuals that in turn permit the serving of targeted ads; given the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals; and given the potentially highly personalised nature of the resulting advertising, it is reasonable to take the view that the information at issue in behavioural advertising not only implicates privacy but also should generally be considered ‘identifiable’ in the circumstances. While such an evaluation will need to be undertaken on a case-by-case basis, it is not unreasonable to generally consider this information to be ‘personal information’.

There are few precedents in Canadian law that have restrained the expansive approach to interpreting personal information.

To varying degrees, privacy laws contain exceptions for business contact information, including the name, title and contact information for a person in a business context. As of June 2015, ‘business contact information’, including the ‘position name or title, work address, work telephone number, work fax number or work electronic address’ of an individual is excluded from PIPEDA.

### iii General obligations for data handlers

As described above, privacy legislation is based on 10 fair information practice principles. This section provides a brief description of the primary obligations for data handlers arising under each of these principles.

**Principle 1 – accountability**

‘An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation’s compliance with the following principles.’

Accountability speaks to the obligations of organisations to establish privacy-related policies and procedures, and to designate staff who are responsible for ensuring that an organisation is compliant with privacy legislation. Organisations are also expected to provide employees with privacy training.

The accountability principle imposes obligations on organisations to ensure that personal information is adequately protected when transferred to a third party for processing. Accordingly, organisations that rely on service providers to process personal information on their behalf (e.g., payroll services) must ensure through contractual means that personal information will be handled and protected in accordance with privacy legislation. This requirement applies equally regardless of whether personal information is transferred to an organisation within or outside Canada.

---

**Principle 2 – identifying purposes**

‘The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.’

Often referred to as providing ‘notice’, organisations are required to document and identify the purposes for collecting personal information. This principle is closely related to the requirement to obtain consent as well as the openness principle.

Notice must be properly targeted to the intended audience. This can pose a challenge as the Commissioner expects organisations to fully explain sometimes complicated technical issues (e.g., OBA) in a manner that is easily understood by any person who may use the organisation’s product or service. It is for this reason that the Commissioner often recommends the use of ‘layered’ privacy notices to explain more technical issues.

**Principle 3 – consent**

‘The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.’

Consent is possibly the single most important and complicated requirement. As a general rule, organisations are required to have consent before collecting, using or disclosing personal information. For consent to be valid under PIPEDA, it must be reasonable to expect that the individual would understand the nature, purposes and consequences of the collection, use or disclosure of his or her personal information.

Consent can either be express or implied. Although the concept is somewhat flexible, ‘express consent’ generally means that a person provides some form of affirmative indication of their consent. It is for this reason that express consent is often equated with ‘opt-in’ consent. Alternatively, as stated in the CSA Model Code, ‘implied consent arises where consent may be reasonably inferred based on the action or inaction of the individual’.

Whether consent can be express or implied depends on a few factors. Express consent is almost always required whenever ‘sensitive’ personal information is involved. This includes, for example, information pertaining to a person’s race or ethnicity, health or medical condition, or financial information (e.g., income, payment information).

The concept of ‘primary purpose and secondary purposes’ is also relevant to the form of consent required. A primary purpose is one that is reasonably necessary to provide a product or service; for example, the collection and use of an individual’s address may be necessary to deliver a product ordered online. In this case, consent would be implied to collect and disclose an individual’s mailing address to a delivery company.

However, marketing or advertising is almost always considered a secondary purpose. For example, an organisation would require express consent to collect and disclose an individual’s mailing address to a third party for the purpose of sending marketing materials.15

---

15 An exception to this rule is PIPEDA Case Summary #2009-008 – Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc under the Personal Information Protection and Electronic Documents Act, in which the Assistant Privacy Commissioner of Canada held that because revenues from advertising allow Facebook to offer a free service, the collection, use and disclosure of personal information for advertising is therefore a ‘primary purpose’, and ‘persons who wish to use the service must be willing to receive a certain amount of advertising’. As such, it is acceptable for Facebook to require users to consent to certain forms of adverts as a condition of using the site.
Note that organisations are prohibited from requiring an individual to consent to the collection, use or disclosure of personal information for a secondary purpose as a condition of providing a product or service.16

A third form of consent, which is sometimes viewed as falling between express and implied consent, is ‘opt-out’ consent. Opt-out consent means that an individual is provided with notice and the opportunity to express non-agreement to a given collection, use or disclosure. Otherwise, consent will be assumed. The Privacy Commissioner has held that it is acceptable to rely on opt-out consent so long as the following conditions are met:

\[ a \] the personal information is demonstrably non-sensitive in nature and context;
\[ b \] the context in which information is shared is limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure;
\[ c \] the organisation’s purposes are limited and well defined, stated in a reasonably clear and understandable manner, and brought to the individual’s attention at the time the personal information is collected;
\[ d \] the organisation obtains consent for the use or disclosure at the time of collection, or informs individuals of the proposed use or disclosure, and offers the opportunity to opt out, at the earliest opportunity; and
\[ e \] the organisation establishes a convenient procedure for opting out of or withdrawing consent to secondary purposes, with the opt-out taking effect immediately and before any use or disclosure of personal information for the proposed new purposes.17

Although exceptions vary among privacy laws, there are a number of exceptions to the need to obtain consent for the collection, use or disclosure of personal information, including the following:

\[ a \] for a purpose that is clearly in the interest of the individual and consent cannot be obtained in a timely way (e.g., emergencies);
\[ b \] for purposes related to law enforcement activities, or to comply with warrants or court orders;
\[ c \] where personal information is ‘publicly available’ as defined under privacy legislation;18 and
\[ d \] in business transactions (e.g., sale of a business), provided that the parties agree to only use and disclose personal information for purposes related to the transaction, protect the information with appropriate security safeguards, and return or destroy the information where the transaction does not go through.

---

16 This is often referred to as ‘refusal to deal’.
18 The definition of ‘publicly available’ is relatively limited under Canadian law. For example, according to the Regulations Specifying Publicly Available Information SOR/2001-7 under PIPEDA, personal information is publicly available if it appears in a telephone directory, business directory, a court or judicial document, or a magazine or newspaper.
Principle 4 – limiting collection

‘The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.’

This principle is relatively simple and self-explanatory: organisations must not collect more information than is required for a stated purpose.

Principle 5 – limiting use, disclosure and retention

‘Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.’

Related to the previous principle, organisations must not use or disclose personal information for purposes beyond those for which the information was originally collected. If an organisation seeks to use or disclose personal information for a new purpose, then consent must be obtained.

Organisations are required to establish clear retention policies and securely destroy information that is no longer necessary. Although it is tempting to retain information indefinitely given the low cost of data storage, a failure to establish retention policies not only risks a violation of this principle, but can substantially increase the risks and costs to an organisation in the case of a data breach.

Principle 6 – accuracy

‘Personal information shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.’

Organisations have an obligation to ensure that personal information is accurate and up to date, the degree of which may depend on the purpose for which the information is used. For example, there may be a heightened obligation to ensure the accuracy of credit information given that this information forms the basis of significant financial decisions about an individual.19

Despite this general obligation, organisations are prohibited from routinely updating personal information where it is unnecessary to do so.

Principle 7 – safeguards

‘Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.’

Organisations are required to implement physical, administrative and technical measures to prevent the loss, theft, and unauthorised access, disclosure, copying, use or modification of personal information.

Canadian law is not prescriptive with respect to safeguards, and specific measures can depend on certain factors, such as the sensitivity of information involved, foreseeable risks and harms, and the costs of security safeguards. That said, certain measures are generally expected by the Privacy Commissioner, including the use of encryption technologies whenever possible.

---

19 The Federal Court emphasised this obligation in Nammo v. TransUnion of Canada Inc, 2010 FC 1284, in which the applicant was denied a loan as a result of information provided by TransUnion that was described as ‘grossly inaccurate’. The Court awarded damages of C$5,000.
and especially where sensitive personal information is involved; limiting access to personal
information to those employees who require access and who are required to sign an oath of
confidentiality; and maintaining audit logs of databases containing personal information.

The Alberta Personal Information Protection Act was the first private sector law
with an explicit requirement to notify individuals in the case of a security breach.\(^{20}\) Once
in force, recent amendments to PIPEDA will require organisations to notify the Privacy
Commissioner and affected individuals of any breach of safeguards if it is reasonable to
believe in the circumstances that the breach poses a real risk of significant harm. Failure
to comply with the new notification requirements once they are in force could result in
a penalty of up to C$100,000.

**Principle 8 – openness**

‘An organisation shall make readily available to individuals specific information about its
policies and practices relating to the management of personal information.’

As stated above, the openness principle is closely related to Principle 2 – identifying
purposes. Most importantly, this Principle requires organisations to provide privacy policies
(or notices). Privacy policies are expected to meet the following requirements:

- **a** provide a full description of what information is collected, used and disclosed, and for
  what purposes;
- **b** be easily accessible, accurate and easily understood by the average person;
- **c** inform an individual of his or her right to access and to request corrections of his or her
  personal information, and how to do so;
- **d** generally describe the security measures in place to protect personal information;
- **e** inform individuals if personal information is transferred to foreign jurisdictions; and
- **f** provide contact information for the organisation’s privacy officer or other person who
  can respond to inquiries about the organisation’s information handling practices.

The Privacy Commissioner also emphasises the value of augmenting privacy notices with
other forms of notice, including ‘just in time’ notices (e.g., through pop-ups and interstitial
pages), layered notices to provide further information about more complex issues for those
who seek such information and icons where applicable (e.g., the ‘Ad Choices’ icon for OBA).

In 2013, the Privacy Commissioner participated in the Global Privacy Enforcement
Network Internet Privacy Sweep, which looked at privacy policies on 326 websites in Canada
and 2,186 websites worldwide, noting concerns in almost half of the Canadian websites.\(^{21}\) In
an example of ‘naming and shaming’, the Privacy Commissioner called out specific examples
of privacy policies considered to be the ‘good, the bad and the ugly’.\(^{22}\)

**Principle 9 – individual access**

‘Upon request, an individual shall be informed of the existence, use, and disclosure of his or
her personal information and shall be given access to that information. An individual shall
be able to challenge the accuracy and completeness of the information and have it amended
as appropriate.’

\(^{20}\) See Personal Information Protection Act, SA 2003, Sections 34.1 and 37.1.


\(^{22}\) http://blog.priv.gc.ca/index.php/2013/08/13/initial-results-from-our-internet-privacy-sweep-
the-good-the-bad-and-the-ugly/.
Organisations are obliged to provide individuals with access to their personal information within a reasonable time frame. This obligation is subject to limited exceptions; for example, organisations may either be allowed or obliged to refuse access where disclosure would reveal personal information about another person; information subject to privilege, trade secrets or confidential information; or information pertaining to law enforcement activity.

Organisations must also allow individuals to request corrections to their personal information. Where such corrections are refused (e.g., information is accurate), an organisation must make a notation on the individual’s file that a correction was requested, and the reason for refusing the correction.

Fees may be charged in some cases, but must be reasonable.

**Principle 10 – challenging compliance**

‘An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation’s compliance.’

Organisations are required to designate a person who can respond to questions and complaints, and establish a process for responding to questions and complaints.

iv  **Technological innovation and privacy law**

Privacy laws are intended to be ‘technologically neutral’, meaning the principles upon which they are based apply equally to all technologies.

However, one technology that has proven particularly challenging is OBA. After years of uncertainty on exactly how Canadian privacy law applies to OBA, some clarity emerged when the Privacy Commissioner published its Policy Position on Online Behavioural Advertising (Policy Position).

As described above, the Privacy Commissioner considers much of the information used for OBA purposes to be personal information. Thus, according to the Privacy Commissioner, PIPEDA (and other privacy legislation) applies to OBA.

However, the Policy Position is generally positive, as it signals that the Privacy Commissioner is willing to accept some form of opt-out consent as sufficient for organisations that use OBA, as opposed to the strict opt-in approach adopted by the European Union.

The Office of the Privacy Commissioner (OPC) has adapted its framework for opt-out consent to OBA, defining the following as a list of conditions:

a. individuals are informed about OBA in a clear and understandable manner at or before the time of collection;

b. organisations should rely on online banners, layered policies and interactive tools. Purposes must be obvious and cannot be ‘buried’ in privacy policies. This includes information about various parties involved in OBA (e.g., networks, exchanges, publishers and advertisers);

c. individuals can easily opt out, ideally at or before the time of collection;

23 For the purposes of this chapter, OBA refers generally to the delivery of advertisements to web browsers that are targeted based on a user’s behaviour online, and the collection, use and disclosure of data for those purposes.

the opt-out takes effect immediately and is persistent;
information is limited to non-sensitive information, to the extent practicable;\(^{25}\) and
information is destroyed as soon as possible or effectively de-identified.

Consistent with past guidance on the issue, the OPC emphasises the need for clear and understandable descriptions of OBA, given the challenges of clearly explaining such a complex issue.

The OPC has published research and guidance in recent years that considers the application of privacy law to other technologies and issues, including facial recognition,\(^{26}\) wearable computing,\(^{27}\) drones\(^{28}\) and genetic information.\(^{29}\)

\[\text{v} \quad \text{Specific regulatory areas}\]

The implementation of CASL in 2014 was one of the most significant privacy-related developments in years. The law establishes rules for sending commercial electronic messages (CEMs) as well as the installation of computer programs, and prohibits the unauthorised alteration of transmission data. Although the majority of CASL came into force on 1 July 2014, the rules that apply to computer programs came into force on 15 January 2015, and will be followed by the private right of action on 1 July 2017.

CASL applies to most forms of electronic messaging, including email, SMS text messages and certain forms of messages sent via social networks. Voice and fax messages are excluded, as they are covered by the Unsolicited Telecommunications Rules. The law applies broadly to any CEM that is sent from or accessed by a computer system located in Canada.

\(^{25}\) In early 2014, the Privacy Commissioner found that Google had violated PIPEDA by using sensitive personal information to target and serve through its AdSense service. Google had allowed its customers to serve targeted adverts for Continuous Positive Airway Pressure devices to internet users identified as suffering from sleep apnoea. Although the Privacy Commissioner has stated that companies can rely on a form of opt-out, implied consent for OBA, adverts targeted at sleep apnoea sufferers did not qualify for this approach given that this involves the collection and use of sensitive, health-related personal information. See Privacy Commissioner of Canada, PIPEDA Report of Findings #2014-001 – Report of Findings: Use of sensitive health information for targeting of Google ads raises privacy concerns, 14 January 2014, www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-001.


A CEM is defined broadly to include any message that has as one of its purposes the encouragement of participation in a commercial activity. This includes advertisements and information about promotions, offers, business opportunities, etc.

CASL creates a permission-based regime, meaning that, subject to a number of specific exclusions, consent is required before sending a CEM. Consent can either be express or implied.

With respect to computer programs, CASL requires any person installing a computer program onto another person's computer system to obtain express consent from the owner or authorised user of the computer system.

CASL is enforced by the Canadian Radio-television and Telecommunications Commission (CRTC). The CRTC has the power to impose administrative monetary penalties for violations of CASL of up to C$10 million per violation.

CASL also includes a private right of action, which allows any person affected by a violation of CASL to sue for actual or statutory damages. The private right of action comes into force on 1 July 2017.

IV INTERNATIONAL DATA TRANSFER

There are no restrictions on transfers of data outside Canada in private sector privacy legislation.30 PIPEDA requires organisations that transfer data to third parties for processing – whether inside or outside Canada – to ensure through contract that the protection provided is ‘generally equivalent’ to the protection that would be provided by the transferring organisation.31 With respect to the potential access to personal information by foreign governments and law enforcement agencies, the Privacy Commissioner has stated that while organisations cannot override or prevent such access through agreements, the law ‘does require organisations to take into consideration all of the elements surrounding the transaction. The result may well be that some transfers are unwise because of the uncertain nature of the foreign regime or that in some cases information is so sensitive that it should not be sent to any foreign jurisdiction.’32

Although consent is not required for transfers to foreign jurisdictions, the Privacy Commissioner has interpreted PIPEDA to require organisations to advise customers (e.g., through privacy policies) that information may be transferred to foreign jurisdictions, and could therefore be accessed by government agencies there.33

---

30 Subject to limited exceptions, public sector bodies in British Columbia and Nova Scotia are required to ensure that personal information in their custody or control is only stored or accessed in Canada; see the Freedom of Information and Protection of Privacy Act, RSBC 1996, Chapter 165, s 30.1, and the Personal Information International Disclosure Protection Act, SNS 2006, c 3, s 5. These laws can pose challenges for service providers located outside Canada that seek to do business with public sector bodies in those jurisdictions.


32 Ibid.

33 Ibid.
The Alberta Personal Information Privacy Act has more explicit requirements when transferring data to service providers outside Canada. Organisations that use service providers to process personal information outside Canada must:

- develop policies that describe the countries to which information is or may be transferred as well as the purposes for which the service provider may collect, use or disclose personal information, and make policies available upon request;\(^{34}\) and
- provide notice to individuals that a service provider outside Canada will collect, use or disclose personal information, and provide information about who can answer questions and where the individual can obtain written information about policies with respect to transfers outside Canada.\(^{35}\)

## V COMPANY POLICIES AND PRACTICES

Companies that do business in Canada are generally expected to have in place the following policies.

### i General

Organisations should:

- establish detailed internal privacy policies for ensuring compliance with privacy legislation that address things such as who is responsible for compliance with privacy legislation;
- establish the various types of personal information collected, used and disclosed, and for what purposes;
- provide training for employees;
- establish administrative, physical and technical security measures for the protection of personal information;
- record transfers of personal information;
- record retention periods and the destruction of personal information;
- record the outsourcing of and third-party access to personal information;
- respond to requests for access to personal information;
- respond to inquiries and complaints about information handling practices; and
- identify and respond to security breaches.

### ii Privacy notices

Organisations must have privacy notices for communicating privacy-related information to the public. This typically consists of an online privacy policy, but can be combined with other means such as written pamphlets, layered privacy notices and just-in-time notifications provided at the point of sale, online and in mobile applications.

### iii Chief privacy officer

Organisations must establish a person who is responsible for compliance with privacy legislation. Further, privacy notices must provide contact information for a person who can respond to inquiries and complaints about information handling practices.

---

34 Personal Information Protection Act, SA 2003, c P-6.5, s 6(1).
VI DISCOVERY AND DISCLOSURE

Privacy laws contain broad exceptions that allow organisations to respond to requests from government agencies for law enforcement purposes, such as in response to a subpoena or warrant, or in response to a court order in a civil proceeding. In addition, private sector organisations can disclose personal information on their own initiative in some circumstances.

There are also several laws that allow government agencies to collect and share information – including personal information – with foreign agencies. For example, the federal government has established bilateral and multilateral conventions for mutual legal assistance with several countries under the federal Mutual Legal Assistance in Criminal Matters Act. Pursuant to these agreements, foreign governments can request information about a specific person, following which the Department of Justice Canada can apply to a court for a warrant compelling disclosure of the information.

There are also other laws that permit transfers to foreign agencies for specific purposes, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the Department of Immigration and Citizenship Act, and the Canadian Security Intelligence Service Act.

Foreign governments cannot directly compel an organisation located in Canada to disclose information. However, personal information about Canadians can be accessed by foreign governments once transferred to those jurisdictions. Canada does not have any ‘blocking statutes’ or specific procedures for resisting access by foreign governments to personal information about Canadians.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Privacy Commissioner of Canada is responsible for the oversight and enforcement of PIPEDA. The Privacy Commissioner is an ‘ombudsman’, meaning that he or she can make recommendations to organisations, but cannot make orders or impose fines. Enforcement is primarily complaint-driven, although the Privacy Commissioner also has the authority to conduct investigations or audits on his or her own initiative. Either a complainant or the Privacy Commissioner can apply to the Federal Court seeking an order, an award of damages, or both. The Privacy Commissioner can also enter into compliance agreements with organisations if the Commissioner believes there has been, or is about to be, a contravention of PIPEDA. The Commissioner can also make public any information obtained in the course of his or her duties if doing so would be in the public interest.

Data protection authorities in Alberta, British Columbia and Quebec have the power to make enforceable orders, which are subject to appeal by provincial courts. Authorities in all jurisdictions (both federal and provincial) have powers to compel evidence.

---

36 RSC, 1985, c 30.
37 SC 2000, c 17.
38 SC 1994, c 31.
39 RSC, 1985, c C-23.
Although damages are possible under private sector privacy legislation, damage awards are not common. One of the largest damage awards to date is C$20,000, which was awarded against Bell Canada for violating PIPEDA in 2013.  

ii Private litigation

Privacy-related litigation has become more common in recent years, as courts are increasingly willing to recognise privacy as a compensable cause of action.

The following four provinces have established a statutory tort for invasion of privacy: British Columbia, Manitoba, Newfoundland and Labrador, and Saskatchewan. A common law tort for invasion of privacy was explicitly recognised for the first time in Ontario in 2012 in Jones v. Tsige. The court awarded relatively modest damages at C$10,000 in that case, stating that damages for privacy invasions should be generally limited to a maximum of C$20,000. In 2016, the Ontario Superior Court cited a new tort referred to as the ‘public disclosure of embarrassing facts’ in a case arising out of the non-consensual publication of intimate images on the internet. The Court awarded damages of C$100,000, which is by far the largest award in a privacy-related case involving a single plaintiff to date.

There have been a growing number of data breach-related class actions in the past few years, involving defendants such as:

a. Home Depot;
b. Bank of Nova Scotia;
c. Human Resources and Skills Development Canada;
d. Health Canada;
e. Durham Region Health; and
f. Rouge Valley Health System.

Although case law involving privacy breach class actions remains limited, precedents arising from class certification and settlement approval proceedings suggest that some courts are sceptical of class actions based on vague allegations of potential harm. For example, in the class action against Home Depot, the court reduced the fees to class counsel previously agreed by the parties, with the court stating that: ‘The case for Home Depot being culpable was

40 Chitrakar v. Bell TV, 2013 FC 1103.
41 Privacy Act, RSBC 1996, c 373.
42 Privacy Act, RSM 1987, c P125.
43 Privacy Act, RSN 1990, c P-22.
45 2012 ONCA 32.
46 Jane Doe 464533 v. ND, 2016 ONSC 541.
50 John Doe v. Her Majesty the Queen, 2015 FC 916.
speculative at the outset and ultimately the case was proven to be very weak.\textsuperscript{53} However, settlements may be much higher where plaintiffs can provide more specific evidence of harm resulting from a breach.\textsuperscript{54}

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Organisations that collect, use or disclose personal information about Canadians are subject to Canadian law, regardless of their location. In response to a complaint about the collection, use and disclosure of personal information by a US-based data broker, the Privacy Commissioner determined that she did not have jurisdiction to compel the company to provide evidence. The Federal Court disagreed, finding that PIPEDA applied to the US data broker, and that the Commissioner did have jurisdiction to investigate because the complainant was Canadian and much of the data had to come from Canada.\textsuperscript{55} The Court noted it was not required to find that PIPEDA applies extraterritorially to reach such a conclusion. It also stated that the fact that an investigation might be ineffective is irrelevant to the legal questions of jurisdiction.

IX CYBERSECURITY AND DATA BREACHES

Canada signed up to the Council of Europe’s Convention on Cybercrime in 2001, but is yet to ratify the treaty. Although there have been repeated attempts over the past decade to pass ‘lawful access’ legislation that would enable Canada to ratify the treaty, legislative proposals have been met with significant opposition. The key aspects of these proposals include new powers for production orders and preservation notices, and requirements that telecommunications service providers (TSPs) make their networks intercept-capable. In addition, proposals have included provisions that would allow law enforcement agencies to compel TSPs to provide customer name and address information without a warrant or court order, which have been most controversial. Mandatory data retention by TSPs has not been a feature of legislative proposals to date.

X OUTLOOK

Privacy-related litigation will continue to grow and should be a top priority for organisations doing business in Canada. Also, Parliament is due to conduct a statutory review of CASL, which could begin as early as autumn 2017. Although the private right of action under CASL has been delayed pending this review, Parliament could decide that the private right of action is necessary and therefore should be brought into effect.

Organisations should also watch for a coming-into-force date for the data breach notification requirements under PIPEDA.

\textsuperscript{53} Lozanski v. The Home Depot, Inc., 2016 ONSC 5447, para. 100.
\textsuperscript{54} For example, in Evans v. The Bank of Nova Scotia, 2014 ONSC 2135 (CanLII), the defendant bank settled for approximately C$1.5 million as some class members suffered identity theft as a result of a data breach.
\textsuperscript{55} Lawson v. Accusearch Inc (FC), 2007 FC 125 [2007] 4 FCR 314.
I OVERVIEW

China does not have an omnibus data protection law as such. In 2005, some legal scholars published a discussion draft for a PRC data protection law, which was reportedly the basis for the State Council draft. However, to date, the State Council has not published the draft data protection law. In fact, data protection law is not included in the 12th National People’s Congress (NPC) legislative plan, which applies to the period 2013–2018.²

Despite the lack of a unified law, China currently has a system of legal rules in place in relation to the protection of personal information, albeit a complicated system. In 2012, the Standing Committee of the NPC issued the Decision on Strengthening Internet Information Protection³ (the NPC Decision), which requires enterprises and, in particular, internet service providers, to protect the personal electronic information of Chinese citizens with several general principles. 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 (MIIT), the State Administration for Industry and Commerce (SAIC), the National Health and Family Planning Commission (NHFPC) and the People’s Bank of China (PBOC) respectively issuing personal protection rules under their own administrative authority over the past few years, and in some circumstances these have overlapped. In the absence of a unified legal definition, ‘personal information’ is defined under many industry-specific rules and generally refers to the information relating to an individual that, alone or in combination with other information, can be used to identify an individual. All these regulations and rules have identified a number of general principles for processing personal information (e.g., personal information collection should follow the principles of legitimacy, appropriateness and necessity, and should be subject to the relevant individual’s consent).

The issuance, on 7 November 2016, of the Cybersecurity Law of the PRC (CSL) is also considered a milestone. The CSL, which became effective from 1 June 2017, includes provisions relating to both cybersecurity protection obligations and data privacy obligations. If an individual’s right to privacy is infringed, the individual may bring a civil lawsuit against the injuring party to seek redress under the Tort Liability Law. Further, sale of personal information or illegal acquisition of personal information may constitute a criminal offence.

---

1 Marissa (Xiao) Dong is a partner at Jun He LLP. Passages of this chapter were originally published in ‘Data Protection Considerations for Commercial Arrangements between the EU and China’, August 2013, and ‘Data Privacy and Security Law Develops Quickly in China’, August 2015.


3 See www.gov.cn/jrzg/2012-12/28/content_2301231.htm.
From a legal point of view, China's personal information legal system is still far less effective and robust than that of the United States or of the EU. It has also long been debated in China whether, in terms of legislation and practice, the country should follow the route of the United States or of the EU. While learning from both models, China has not yet committed to one or other of these approaches, and in fact the Chinese way, as it has been formed in practice, is somewhat of a mixture of both. With a view to cracking down on the serious abuse of personal information, Chinese legislators have introduced a broader scope of personal information offences in the recently promulgated amendment to the Criminal Law. Furthermore, in judicial practice, in a recent civil case, Ms Zhu Ye v. Baidu, the Chinese court ruled that the use of cookies by internet service providers, and accordingly delivering targeted advertising, does not violate the right of privacy of Chinese citizens, which has been read by the press as a judgment in favour of the 'new economy'. Chinese companies and multinationals in China are gradually paying more attention to their practice of collection and utilisation of personal information in China, with some promoting industry-specific standards to provide guidance in the still comparatively grey areas.

In brief, although from an overall perspective the abuse of personal information is still a very serious reality, and people living in China still suffer unsolicited calls, emails and text messages, the attitude and rules of the governmental authorities, the practice of companies, the understanding of courts and, more importantly, public awareness are changing in a fast and sometimes dramatic fashion in this information era, which is unlike anything that any other nation, or even the world, has previously experienced.

II THE YEAR IN REVIEW

The most important legislative development in 2016 and 2017 is the formal issuance and entry into force of the CSL and a number of ancillary regulations, rules and national standards, either formally issued or still at the draft stage. The CSL and ancillary legislation will provide a new legal framework for the protection of cybersecurity and personal information in China.

The CSL applies to the construction, operation, maintenance and use of networks, as well as to the supervision and administration of cybersecurity within the territory of the PRC. 'Networks' include networks and systems composed of computers, other information terminals and relevant facilities used for the purpose of collecting, storing, transmitting, exchanging and processing information in accordance with certain rules and procedures (Article 76). 'Network operators', an important subject of legal obligations under the CSL, are broadly defined as 'owners and administrators of networks and network service providers' (Article 76). Pursuant to the CSL, 'safeguarding national cyberspace sovereignty' is a fundamental principle and, for that purpose, it includes provisions on, inter alia, the strategy, plan and promotion of cybersecurity, network operation security, network information security and alarm and emergency response systems.

Ancillary regulations issued include, primarily, the Measures on Security Review of Network Products and Services (Trial for Implementation), the Regulations on Security Protection of Critical Information Infrastructures, the Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data. Various national standards (such as the Information Security Technology Guidelines for Cross-Border Data Transfer Security Assessment and the Personal Information Security Guidance) that are considered to have a potentially significant impact on the operation of companies in China are still at the draft stage.
Government enforcement is also greatly strengthened, with the issuance of the CSL affecting different governmental authorities, including the Cyberspace Administration of China (CAC) and the Ministry of Public Security, and precipitating the inspection of critical information infrastructure (CII) and investigations into failure to comply with classified security protection systems. Cybersecurity law has become a widely discussed topic in China this year and many companies have started programmes in readiness for compliance with the CSL.

### III REGULATORY FRAMEWORK

China's regulatory framework for personal information protection includes laws and regulations in the criminal, civil and administrative areas.

#### 1 Privacy and data protection legislation and standards

**CSL**

The CSL provides various security protection obligations for network operators, including, *inter alia*:

- compliance with a series of requirements of tiered cyber protection systems (Article 21);
- verification of users' real identity (an obligation for certain network operators) (Article 24);
- formulation of cybersecurity emergency response plans (Article 25); and
- assistance and support to investigative authorities where necessary for the protection of national security and investigation of crimes (Article 28).

The CSL, for the first time under PRC law, clearly imposes a series of heightened security obligations for critical information infrastructure operators (CIIOs), including:

- internal organisation, training, data backup and emergency response requirements (Article 34);
- storage of personal information and other important data must be secured within the PRC territory, in principle (Article 37);
- procurement of network products and services that may affect national security must pass the security inspection of the relevant authorities (Article 35); and
- annual assessments of cybersecurity risks and reports on the results of those assessments and improvement measures to be submitted to the relevant authorities (Article 38).

As regards personal information, the CSL reiterates the obligations of network operators regarding the protection of personal information that appear across existing laws and regulations, including the mandate to observe the principle of lawfulness, necessity and appropriateness in the collection and use of personal information and to observe the ‘inform-and-consent’ requirements (Article 41), to use personal information only for the purpose agreed upon by the relevant individual (Article 41), to adopt security protection measures for personal information (Article 42), and to protect the individual’s right to access and correct personal information (Article 43). In addition, the CSL also incorporates some new rules on personal information protection, including data breach notification requirements (Article 42), and data anonymisation as an exception for inform-and-consent
requirements (Article 42), and the individual’s right to request that network operators make corrections to or delete their personal information if the information is wrong or used beyond the agreed purpose (Article 43).

Criminal offence

Article 253 of the Criminal Law (as provided in Amendment VII to the Criminal Law)\(^4\) applies where any individual (including staff of governmental authorities and companies engaged in industrial sectors, including finance, telecommunications, transportation, education and healthcare) sells or illegally provides personal information obtained in his or 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 and other individuals directly responsible for the criminal activity are subject to the punishments listed above.

Amendment IX to the Criminal Law,\(^5\) which became effective from 1 November 2015, has amended Article 253, and has broadened the scope of personal information-related offences and increased legal liability.

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

Tort liability

The Tort Liability Law,\(^6\) effective as of 1 July 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 right and including the right of privacy. This is 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. An injured party can seek redress against the injuring party.

Industry-specific regulations and rules

The NPC Decision, as mentioned above, has set forth a number of important principles for handling personal electronic information. It is also important to note that the Consumer Rights Protection Law,\(^7\) effective as of 15 March 2014, includes and echoes the requirements of the Decision.

---


\(^7\) See www.saic.gov.cn/zcfg/fl/xxb/201310/t20131030_139167.html.
Accordingly, various governmental authorities have issued their respective administrative regulations and rules to set out more specific requirements in their area – including, for example, MIIT, SAIC, NHFPC – and to provide rules for a number of different types of personal information. For example:

a. users’ personal information collected by telecom and internet operators in their business operations;

b. operators’ and users’ personal information collected in the course of e-commerce platforms’ business; and

c. population health information collected by healthcare organisations and entities.

ii General obligations for data handlers

In brief, data handlers generally have to obey the following principles:

a. complying with the principles of lawfulness, fairness and necessity when collecting and using personal information;

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

c. publishing statements describing the collection and use of data subjects’ personal information;

d. keeping personal information strictly confidential, and refraining from disclosing, selling or illegally providing such information to others;

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

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

iii Technological innovation and privacy law

Chinese law does not generally prohibit the use of online tracking and behavioural advertising, cloud computing and big data, and as mentioned in Section II, the government is actively promoting such technological innovation in China to facilitate growth in the industry. Nevertheless, many issues still lack clarity under the law, and this legal ambiguity has, in practice, brought about uncertainty for business operators, particularly where the adoption of new types of technology or business model are concerned.

Cookies

The use of cookies is a good example of the above-mentioned issues, and there have been contradictory views around key aspects of the use of cookies. On 15 March 2013, World Consumer Rights Day, the Chinese Central Television Station specially reported that consumers’ personal information was being divulged when they surfed the web, and accused many websites of prying into internet users’ privacy. The report caused widespread public panic. Although many industry participants sought to clarify the facts around the use of cookies, many people were still not clear about how cookies work exactly and whether indeed their privacy had been invaded. From a legal point of view, many issues are not clear because of the lack of detailed rules. For example, the specific reference of the consent

---

8 See finance.qq.com/a/20130315/007380.htm.
requirement for the purpose of utilising the personal information of individuals is not clear under certain circumstances, whether implied consent is sufficient in all scenarios, or to what extent business operators must disclose to users or consumers details of proposed future use of information collected. The Chinese Advertising Association is actively promoting industry standards for targeted advertising and mobile internet advertising,9 and it is still waiting to see whether these standards will be widely accepted and implemented in practice.

In the first civil case regarding internet advertising and the online collection and use of personal information, involving Chinese search engine giant Baidu, a Ms Zhu claimed that Baidu’s targeted advertising on its partners’ websites, using cookies set when she used the search engine, infringed her right to privacy. Interestingly, the appellate court’s judgment contrasted with the opinions of the court of first instance in many aspects. The appellate court decided three important points at variance with the judgment of the court of first instance: that the information collected by Baidu cookies does not contain personal information under PRC law; that the network user does not suffer cognisable injury by receiving targeted adverts on websites within Baidu’s advertising alliance; and that the notification and consent mechanism provided on Baidu’s search engine website is legal and sufficient. Although the Chinese court judgment does not have a binding effect, it provides important guidelines and may affect other similar cases in the future.

Cloud computing

Cloud computing has posed new challenges to the law, in particular because it is not completely transparent as to where and how the information is stored and processed in ‘the cloud’, or how prevention of hacker attacks and the security of information stored in the cloud may be assured. As mentioned in the Opinions for Promoting Creative Development of Cloud Computing and Fostering a New Sector of Information Industry issued by the State Council, China is faced with various issues with respect to cloud computing, along with development opportunities. These issues include lack of service capacity and core technology, insufficient sharing of information resources and high levels of information security risk. In the Opinions, the State Council’s demands include:

a facilitating research into applications of personal and enterprise information in a cloud computing environment;

b promulgation of laws and systems relating to information protection;

c rules relating to collection, storage, transfer, deletion and international transfer of information; and

d information security law.

iv Specific regulatory areas

Many different specific types of personal information are governed under different sets of laws and administrative rules, and some of these provisions overlap. A few common types of personal information are listed below.

---

**Users’ personal information in telecom and internet services**

‘Users’ personal information’ in telecom and internet services is defined under the Provisions on the Protection of Personal Information of Telecommunications and Internet Users (the Protection Provisions) of July 2013.10 The Protection Provisions stipulate several measures that telecommunications and internet service providers should take internally for the prevention of leakage, damage or loss of personal information of users. The Protection Provisions also provide that telecommunications authorities should check how telecommunications and internet service providers protect personal information during the annual inspection in respect of their telecommunications licence.

**Population health information**

‘Population health information’ is stipulated under the Administrative Measures for Population Health Information (for Trial Implementation),11 effective on 5 May 2014, as information generated and collected in the course of service and administration by medical, healthcare and family planning services agencies. The collection and handling of population health information is subject to specific rules, and such information is particularly prohibited from being stored outside China.

**Personal financial information**

Financial institutions, including banks, insurance companies, securities companies and similar organisations, are required to preserve client information that they obtain in the course of business operations under the Administrative Measures Regarding the Retention by Financial Institutions of Customer Identification Documents and Materials and Transaction Records.12 Financial institutions in the banking industry are subject to more specific requirements under the Notice of Strengthening the Work Relating to the Protection of Personal Financial Information by Financial Institutions in the Banking Industry issued by the PBOC.13 ‘Personal financial information’ is defined as information that is obtained, processed and retained by financial institutions during their business operations, or through their access to the credit information system of the PBOC, payment systems and other systems that include:

a personal identification information;
b information pertaining to personal property;
c information pertaining to personal accounts;
d personal credit information;
e information pertaining to personal financial transactions;
f derived information, such as personal consumption habits and investment intentions, which can reflect certain situations of the individual and are formed by handling and analysing the relevant raw information; and
g other information obtained and preserved during the course of establishing a business relationship with the relevant individual.

---

10 See www.gov.cn/zhengce/2013-07/19/content_2451360.htm.
12 See www.gov.cn/zhengce/content/2007-06/22/content_658488.htm.
13 See www.gov.cn/zhengce/content/2011/content_1918924.htm.
IV INTERNATIONAL DATA TRANSFER

Although at present there are no specific legal requirements for the transfer of personal information within China itself, the cross-border transfer of personal information from China to other jurisdictions is subject to the general privacy requirements under civil law. Where the personal information to be transferred is of a specific nature, there are also explicit requirements under industry-specific regulations and rules.

For example, in the heavily regulated banking industry, the processing of personal information collected by commercial banks is administered by stringent rules. The PBOC especially requires that personal financial information collected in China must be stored, handled and analysed within the territory of China and, unless otherwise stipulated, banks are not allowed to provide domestic personal financial information overseas. Another example is the transfer of employee information, which is very sensitive in practice and requires delicate handling despite the provisions regarding employee information being comparatively simple at present.

In addition to stipulations under civil law and industry-specific regulations, disclosing information to an offshore entity is strictly prohibited if the information involves PRC state secrets. This issue has become highly sensitive where Chinese subsidiaries of US companies and companies listed in the United States are requested to provide information to the US authorities or US affiliates in relation to internal Securities and Exchange Commission investigations, or where foreign companies are conducting internal investigations (e.g., for Foreign Corrupt Practices Act purposes) and their Chinese subsidiaries need to transfer documents overseas. Under the State Secrets Protection Law (2010)\textsuperscript{14} and the Measures for Implementing the State Secrets Protection Law (2014),\textsuperscript{15} no documents or materials containing state secrets are allowed to be carried, transmitted, posted or transported outside China without approval from the competent governmental authorities. However, the term ‘state secrets’ is broadly defined, covering extensive matters such as major decisions on state affairs, national defence and activities of the armed forces, diplomatic activities and foreign affairs, national economic and social development, science and technology, activities safeguarding national security, and the investigation of criminal offences. The lack of an explicit list or guidelines specifying what information constitutes state secrets, or procedures to recognise state secrets, have contributed, in practice, to extreme difficulty in dealing with information that might be considered as containing state secrets.

Furthermore, the Information Security Technology Guide for Personal Information Protection within Information Systems for Public and Commercial Services\textsuperscript{16} (the Guidelines) was issued on 15 November 2012, and became effective from 1 February 2013. The Guidelines, however, do not serve as a statutory law but as a non-mandatory national standard. Nevertheless, as many important internet service providers have been participating in the process of their drafting, the Guidelines are expected to be observed, or at least used as reference in establishing internal rules, by many industry participants, and some believe the Guidelines may serve as a basis for future legislation on personal information protection. The Guidelines set out both general principles and specific requirements with respect to the collection, processing, transmission, utilisation and management of personal information in

\textsuperscript{14} See www.gov.cn/flfg/2010-04/30/content_1596420.htm.

\textsuperscript{15} See www.gov.cn/zwgk/2014-02/03/content_2579949.htm.

\textsuperscript{16} See tech.qq.com/a/20110211/000264.htm.
various information systems. In particular, in respect of cross-border transfers of data, the Guidelines provide that in the absence of explicit law or regulation, and without the approval of the industry administrative authority, a Chinese data controller should not transfer any personal information to a data controller registered overseas. Although this recommendation is not mandatory, it reflects the attitude of the governmental authorities that have participated in the issuance of the Guidelines, and we would expect there may be increasingly strict legal requirements in this regard in the future.

Notably, CAC released a draft of the Measures on Security Assessment on the Cross-Border Transfer of Personal Information and Important Data for public comment and it has yet to be finalised. The Draft requires, in addition to the data localisation and security assessment on CIIOs, that all ‘network operators’ should also carry out security assessments for cross-border transfers of personal information and important data collected and produced by them in the course of their operations within China. The Draft regulates cross-border data transfers by way of both ‘self-assessment’ and assessment by authorities. In brief, network operators are required to carry out self-assessment for all cross-border transfers of data, while cross-border transfers of data satisfying certain tests must be submitted to the applicable industrial regulatory authority or the national cyberspace authority for assessment.

The National Information Security Standardisation Technical Committee (TC 260) released a draft of the Information Security Technology Guidelines for Cross-Border Data Transfer Security Assessment for public comment (and a second draft has already been released). As an important ancillary document to the CSL, the Guidelines put forward detailed recommendations on the assessment process, assessment methods and points regarding the data export security assessment. Although the Guidelines do not have mandatory legal force, they may be adopted and referred to in data export activities by network operators in various industries, since existing laws and regulations fail to provide detailed guidance. In data export assessments, enterprises need to comprehensively take into account factors such as the consent of the individuals whose personal data is being exported, the necessity for the data export, the security protection measures of the data exporters and data recipient, and the political and legal environment of the receiving country or region.

V COMPANY POLICIES AND PRACTICES

Following the entry into force of the CSL in China, companies have started to consider and adopt rules for the collection and processing of information obtained both in the course of their business and from their employees’ personal information, and also rules regarding their cybersecurity protection practices.

Under the CSL, it is provided that a CIIO must designate a person with specific responsibility for security management organisation and security administration, and carry out a security background check on that responsible person and on relevant personnel holding key positions. Network operators are required to appoint personnel responsible for cybersecurity protection. Although not specifically mentioned, telecom and internet service providers are required to set up a security officer post, and they are also required by the MIIT to specify the responsibilities of each department, post and branch in terms of managing the security of users’ personal information, and to establish work processes and security management systems for the collection and use of users’ personal information and related activities.
VI DISCOVERY AND DISCLOSURE

In practice, discovery and disclosure issues mainly arise out of cases involving cross-border investigations or litigation. For example, a subsidiary of a US company in China may be required to produce documents when the US company is ordered to produce information on the basis of a subpoena, or a Chinese company may also be subject to such a requirement if the company is sued in the United States. There will be complex state secret and personal information issues involved in the discovery and disclosure process, and a Chinese lawyer’s legal opinion is normally sought to ensure that the process is carried out in compliance with PRC law. Again, because of the lack of explicit rules, such a process can be challenging and tricky, and may involve communication with different Chinese governmental authorities. Cross-border transfer requirements pursuant to the CSL will also need to be taken into consideration.

VII PUBLIC AND PRIVATE ENFORCEMENT

China does not have a central privacy regulator, and many governmental authorities regulate privacy issues within their own delegated area of authority (normally a specific industry sector), and these areas may overlap. For example, the MIIT is in charge of telecom and internet service providers, the SAIC administers market order, consumer rights protection and advertising issues, and the PBOC is in charge of the administration of personal financial information. Although there have been sanctions imposed by the SAIC and the PBOC in certain localities for the leaking or abuse of personal information, there have been no milestone cases yet. CAC is the designated enforcement authority for the CSL and following the entry into effect of the CSL it has already been active, starting investigations into practices in this area.

There have already been various privacy lawsuits, even before the Tort Liability Law became effective, and at that time claims were brought for infringement of the right to reputation. However, there is still no unified interpretation of what constitutes privacy of individuals and what circumstances would be treated as infringements of privacy rights. Although many judgments rendered by local courts have provided their views and guidance on this matter, these cases are not legally binding. There are still controversial views held by different local courts on this matter.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Strictly from a legal point of view, the rules for handling personal information only apply to businesses operating within Chinese territory. However, in this high-tech era, the boundaries of business blur, and sometimes it is unclear and uncertain how these rules would apply, in particular when, as is the case on many occasions, cross-border business such as e-commerce is involved. Foreign organisations operating on the internet in a Chinese market and with Chinese customers as their main target would still have to consider whether they are required to set up a presence in China as a first step for the business and, subsequently, whether they would need to follow Chinese data protection rules. The CSL and its ancillary rules, in particular the draft measures and guidelines for cross-border data transfer, will also pose new challenges for foreign organisations with operations in China.
IX CYBERSECURITY AND DATA BREACHES

In April 2014, to respond to the various challenges in the new era, President Xi Jinping for the first time raised the ‘overall concept of national security’. Thereafter, a series of pieces of legislation relating to national security was put on an accelerated track, including the National Security Law (NSL), the Counter-Terrorism Law (CTL) and the CSL. The CTL, NSL and CSL all include, or are likely to include, provisions relating to information and technology security, and have drawn wide attention from foreign companies, especially high-tech and internet companies that have operations in China.

On 1 July 2015, China’s legislature, the NPC Standing Committee, passed the NSL, and it came into effect on the same date. The NSL, for the first time, provides for ‘safeguarding the national cyberspace sovereignty’, and adds cybersecurity and information security as important parts of national security, in contrast with the former NSL, which focused primarily on counter-espionage. The NSL further requires the state to establish a national security review system to review matters and activities that influence or may influence national security, including those relating to network information technology products and services.

The CTL was enacted at the end of 2015. The CTL is the first counter-terrorism law in China that includes wide-ranging stipulations and is intended to cover all aspects of counter-terrorism activities. The CTL provides, inter alia, obligations for telecom and internet enterprises to cooperate with government authorities in investigating terrorism activities, which may have a significant impact on the operation of internet and tech firms in China. For example, according to the CTL, telecom and internet service providers are required to provide technical interfaces and technical assistance in decryption and other efforts to public and national security authorities engaged in the lawful conduct of terrorism prevention and investigation. However, the provisions of the CTL still lack details as to how these requirements will be implemented, which remains to be seen in practice.

As mentioned above, the CSL entered into effect on 1 June 2017 and has become the fundamental law in China for the protection of cybersecurity and personal information.

X OUTLOOK

As with the rest of the world, in China, threats to cybersecurity have been the subject of more intense focus by governmental authorities and public and private companies. Over the past few years, there has been an increase in China in the amount of legislation regarding personal information protection and cybersecurity law, and how these new laws and regulations will be implemented remains to be seen.

The CSL is considered a legislative milestone in China in this field. The CSL is the first law in the PRC specially focused on cybersecurity matters. With the entry into effect on 1 June 2017 of the CSL, internet companies and other industries in China are now subject to a wide array of stricter, more comprehensive obligations, and face more severe punishments for violations. As an omnibus law on cybersecurity issues, the CSL has many provisions that are still very general and abstract, and the detailed requirements for implementation and enforcement depend on subsequent and more specific implementation regulations, and on opinions from relevant authorities. We can expect the relevant regulatory authorities to continue to promulgate series of implementation regulations to clarify certain requirements under the CSL, such as regulations on tiered cybersecurity protection systems, the specific scope and protection measures regarding CII, the protection of minors on networks, the
mandatory security certification and the test requirements for key network devices and special cybersecurity products, and national security reviews of the network products and services procured by CIOs.

In view of these legislative changes, companies will have to consider whether they need to adjust their business operations and practices accordingly and enhance their cybersecurity protections to ensure full compliance with the CSL. Given that the specific details of implementation of the CSL requirements are not yet entirely clear, companies will also have to follow closely any subsequent releases of regulations and opinions by the relevant governmental authorities.
Chapter 10

FRANCE

Arnaud Vanbremeersch and Christophe Clarenc

I OVERVIEW

The French data privacy rules are a transposition of the Data Protection Directive. The General Data Protection Regulation (GDPR), which will replace the Data Protection Directive as from 25 May 2018, will be applicable on French territory without transposition measures being necessary. In the meantime, data privacy remains regulated for the most part by Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (the Data Protection Law).

Compliance with the French data protection framework remains of concern for companies given the penalties imposed by the French data protection authority (CNIL) and reputational risks.

Following a number of high-profile cyber-attacks, cybersecurity has become a priority for administrations and companies alike, with a particular focus on vital sectors and on interception products. Terrorist attacks have also resulted in increased awareness of national security issues and of the need to better protect information systems.

Cybersecurity in France is governed by an ever increasing number of laws and orders, and is supervised by the French Network and Information Security Agency (ANSSI), the French digital security agency.

As a member of the European Union, France will need to implement the NIS Directive before 9 May 2018, but has already identified vital sectors subject to specific cybersecurity rules.

1 Arnaud Vanbremeersch is a partner at Duclos, Thorne, Mollet-Viéville & Associés (DTMV) and Christophe Clarenc is an independent lawyer working with DTMV. This is an updated version of last year’s chapter.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

II THE YEAR IN REVIEW

On the data privacy front, the year was marked by the amendment of the Data Protection Law by Law No. 2016-1321 of 7 October 2016, known as the Digital Republic Act (DRA),\(^4\) some provisions of which anticipate the GDPR:

\( a \) regarding individuals’ rights: the DRA establishes the principle of control by the individual of his or her data,\(^5\) the right to be forgotten for minors,\(^6\) the option for individuals to organise the fate of their personal data after their death\(^7\) and the option for individuals to exercise their rights electronically;\(^8\)

\( b \) regarding transparency of data processing: the DRA establishes that information should be available to individuals on how long their data will be kept;\(^9\)

\( c \) regarding the CNIL’s jurisdiction: the DRA strengthens the CNIL’s sanctioning power and provides for more systematic consultation of the CNIL; and

\( d \) regarding the opening of public data: the DRA has established a rapprochement between the CNIL and the CADA.\(^10\)

In addition, the CNIL announced that a list of the formalities carried out since 1979 by data controllers (public and private) using files dealing with personal data would be soon available on its website.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

French Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties is still the cornerstone of data protection in France and has been amended multiple times since its inception, most recently by the DRA.


\(^4\) Law No. 2016-1321 of 7 October 2016.
\(^5\) Article 1 of the Data Protection Law.
\(^6\) Article 40 of the Data Protection Law.
\(^7\) Article 40-1 of the Data Protection Law.
\(^8\) Article 43 bis of the Data Protection Law.
\(^9\) Article 32 of the Data Protection Law.
\(^10\) Commission on Access to Administrative Documents.
The LCEN\textsuperscript{13} and Decree No. 2011-219 of 25 February 2011\textsuperscript{14} regulate the processing of personal identification, location and traffic data of individuals contributing to the creation of online content.

**Key definitions under French standards**

\(a\) Data controller: unless expressly designated by legislative or regulatory provisions relating to processing, a data controller is a person, public authority, department or any other body that determines the purposes and means of data processing;\textsuperscript{15}

\(b\) data subject: an individual to whom the data covered by the processing relate;\textsuperscript{16}

\(c\) data processor: a person who acts under the authority of the data controller or of the processor or any person who processes personal data on behalf of the data controller;\textsuperscript{17}

\(d\) personal data: any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to them;\textsuperscript{18}

\(e\) processing of personal data: any operation or set of operations in relation to such data – by whatever mechanism – especially obtaining, recording, organising, storing, adapting, altering, retrieving, consulting, using, disclosing via communication, disseminating or any other making available, aligning or combining, blocking, deleting or destroying;\textsuperscript{19}

\(f\) recipient of processing of personal data: any authorised person to whom the data are disclosed, other than the data subject, data controller, subcontractor and persons who, through their work, are in charge of processing data, except legally entitled authorities that in particular situations ask the data controller to send them the personal data concerned; and

\(g\) sensitive personal data: personal data that reveals, directly or indirectly, the racial and ethnic origins, political, philosophical, religious opinions or trade union affiliation of persons, or their health or sexuality.\textsuperscript{20}

**Data protection authority**

The CNIL is the independent administrative authority responsible for ensuring personal data protection.\textsuperscript{21} For this purpose, the CNIL has significant powers, including in a supervisory capacity and the power to impose penalties, and these were strengthened by the DRA. CNIL members and accredited officers have access – from 6am to 9pm – for the exercise of their functions to the places, premises, surroundings, equipment or buildings used for the

\textsuperscript{13} Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy.
\textsuperscript{14} Decree No. 2011-219 of 25 February 2011 on holding and communicating data to identify any person contributing to creation of online content.
\textsuperscript{15} Article 3 of the Data Protection Law.
\textsuperscript{16} Article 2 of the Data Protection Law.
\textsuperscript{17} Article 35 of the Data Protection Law.
\textsuperscript{18} Ibid.
\textsuperscript{19} Ibid.
\textsuperscript{20} Article 8 of the Data Protection Law.
\textsuperscript{21} Article 11 of the Data Protection Law.
processing of personal data for professional purposes. Penalties for non-compliance are as high as €3 million. Penalties are often published by the CNIL, which conducts about 500 checks per year.

As a regulator, the CNIL authorises the processing of information regarding a subject’s politics, philosophy, medical state and sexuality, genetics, offences, waiver of rights, combination, social security number, social difficulties and biometric data. The French authority also receives notifications relating to other processing.

The CNIL is empowered to transfer information to authorities exercising similar powers in non-member States of the European Union if these States provide an adequate level of data protection.

ii General obligations for data handlers

Data controllers must comply with the five essential data protection principles set out below.

Collection

Personal data must be collected and processed fairly and lawfully. Data should not be collected without the knowledge of the data subject. The data controller must provide the data subject with the information required by Article 32 of the Data Protection Law. The data subject’s consent must be obtained except when, for example, data processing:

a) complies with any legal obligation to which the data controller is subject;

b) is necessary to protect the data subject’s life;

c) is necessary for the execution of either a contract to which the data subject is a party or steps taken at the request of the data subject before entering into a contract; or

d) pursues a legitimate interest for the data controller or the data recipient, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

Processing

Data must be processed for specified, explicit and legitimate purposes. The legitimacy of the processing of personal data is assessed in particular in the light of French legislation and the data subject’s individual rights. Data cannot subsequently be processed in a manner that is incompatible with such purposes. Nevertheless, further data processing for statistical, scientific and historical purposes may be considered legitimate.

Nature of processed data

Data must be adequate, relevant and not excessive in relation to the purposes for which it is obtained and to further processing. Data must be accurate, complete and up to date.

Data storage

Data must be stored for a period no longer than is necessary for the purposes for which the data are collected and processed. The data controller is now required to inform the data

---

22 Article 47 of the Data Protection Law.
23 New Article 49 bis of the Data Protection Law.
24 Articles 6, 7, 23, 24 and 32 of the Data Protection Law.
subject about the duration of the storage of the processed data or, if that is not possible, the criteria used to determine this duration. The provisions requiring all data to be stored in the EU were removed from final version of the DRA.

Requirements for processing data
The data controller must complete all necessary formalities before processing data.

Data controllers called upon to process personal data must notify the CNIL. Simplified notifications can be communicated if the data processing complies with the relevant standard established and published by the CNIL. An authorisation application must be submitted to the CNIL in special cases, such as the processing of:

- political, philosophical, medical and sexual information on a subject;
- genetic data, offences, waivers of a personal right;
- combinations;
- social security numbers;
- social difficulties; and
- biometrics.

Moreover, data transfers outside the EU are generally subject to the authorisation procedure. A data controller not established in France, or any other EEA country, but using equipment in France to process personal data other than merely for the purposes of transit in France, has to appoint a representative in France.

Some data processing is exempt from formalities. This is true for any data processing subject to standards drawn up and published by the CNIL or processing for which the data controller has appointed a personal data protection officer charged with independently ensuring compliance with the obligations of the Data Protection Law, except for data transfer outside the European Union. Currently, there are no legal requirements under French law to appoint a data protection officer, even if the CNIL strongly recommends this.

Minors
Where the data subject concerned was a minor at the time of data collection, he or she can obtain the erasure of the problematic data ‘as soon as possible’.

iii  Technological innovation and privacy law

Anonymisation
Anonymous data do not fall within the scope of the French Data Protection Law. However, the CNIL considers that perfect anonymisation must be irreversible. This means that all information identifying an individual directly or indirectly is removed so that it will be impossible to re-identify this person. For example, the CNIL recommends generating a secret code that is too long and difficult to memorise, and applying a one-way function to the data.26

The anonymisation of sensitive data is submitted to the CNIL for authorisation.27

---

25 Article 40 of the Data Protection Law.
26 2010 Personal Data Security Guide.
27 Article 8-III of the Data Protection Law.
**Big data**

Although big-data processing is not prohibited, the CNIL pays particular attention to big data processed for the purpose of marketing or tracking without the knowledge and the consent of the data subject. The CNIL is especially concerned about connected objects, ‘self-quantified’ data (data provided by the individuals themselves28 but hosted by a data controller who has access to sensitive data), and new devices that store a significant amount of data without security and confidentiality guarantees and without transparency for users.

**Bring your own device**

The CNIL considers that the use by employees of personal devices at work presents a risk of breach of privacy for the employee and the security of his or her data. The relevant data controller must take technical and practical measures to ensure the protection of employees’ privacy and data.

**Cloud computing**

The CNIL considers that data subjects suffer from a lack of transparency on the part of cloud service providers, and more especially in terms of security and transparency. According to the CNIL, data subjects generally do not know whether their data are transferred or to which country. In June 2012, the CNIL published recommendations for companies planning to use cloud computing services. The CNIL also describes the essential items that should appear in a cloud computing service contract.29

**Cookies and similar technologies**

Article 32-II of the Data Protection Law regulates the use of cookies and, in Resolution No. 2013-378 of 5 December 2013, the CNIL adopted a recommendation on cookies and other trackers.

Data subjects must be informed in a clear and comprehensive manner by the data controller. Moreover, data subjects must give their prior consent to the implementation of cookies within their device (computer, smartphone, tablet, etc.). Consent is not required for cookies exclusively intended to enable or facilitate communication by electronic means or for cookies strictly necessary for the provision of an online communication service at the user’s express request.

The CNIL has recently extended its controls, in particular to 13 third-party cookie transmitters established in France and the United States. The CNIL considers that the site publishers are the only ones able to provide direct information on the cookies deposited on the terminals of the internet users, whose visit triggers the deposit of the cookies. Whether these site publishers are processors or subcontractors, it is up to them to provide the internet users with information on the groups of cookies deposited and the means available to users to refuse the cookies.

28 Device enabling measurement and analysis of your own personal data.

**Password security**


The requirements of the CNIL are related to password authentication, authentication security, password storage and password renewal or recovery.

**Privacy of private electronic correspondence**

Decree No. 2017-428 of 28 March 2017 concerns individuals and companies providing private electronic correspondence services, and it imposes a time limit of a year for the periodicity of the collection of the express consent of the user.

**iv Specific regulatory areas**

**Whistle-blowing – biometric devices**

Whistle-blowing procedures are subject to CNIL authorisation. The CNIL has published a standard that allows data controllers to process a simplified notification if they comply with the framework provided by this standard. Its scope was extended in July 2017, following the new Law No. 2016-1691 of 9 December 2016. It now covers all professional fields, except defence, health (medical confidentiality) and legal (attorney–client privilege) services.31

Biometric devices identifying individuals by their behavioural, physical or biological characteristics are subject to special CNIL control and cannot be implemented without its prior authorisation. The French authority has published standards applicable to certain biometric devices that allow data controllers to process a simplified notification if they comply with the framework provided by the CNIL’s standard. The CNIL has, for example, published standards relative to hand contour recognition to control workplace access32 and fingerprint recognition to control workplace access.33

**Electronic marketing**

Electronic marketing is regulated by the LCEN34 and Decree No. 2011-219 of 25 February 201135 on the processing of identification, location and traffic data relative to persons creating online content.

Electronic marketing is possible provided that consumers have given their explicit consent to be contacted at the time of the collecting of their email address.

Consent is not required if the consumer is already a customer of the company and if the products or services proposed to the consumer are similar to those already provided by

---


31 https://www.cnil.fr/fr/alertes-professionnellesmodification-de-lautorisation-unique-ndegau-004.


35 Decree No. 2011-219 of 25 February 2011 on holding and communicating data to identify anyone contributing to the creation of online content.
the company. The customers concerned must – at the time of the collection of their email address – be informed that their email address will be used for electronic marketing, and they must be able, freely and easily, to oppose the use of their email address for this purpose.

Two professional electronic marketing ethics codes have been recognised by the CNIL in accordance with the Data Protection Law.\(^{36}\)

**Health**

Article L1111-8 of the Public Health Code provides that personal health data collected or produced during prevention, diagnosis or treatment activities must be hosted by accredited hosting providers. The Ministry of Health publishes the list of accredited hosting service providers. Foreign hosting providers may also be subject to the approval procedure.

**IV INTERNATIONAL DATA TRANSFER**

Data controllers may not transfer personal data to a country that is not a Member State of the European Union if the country is not considered, by the European Commission, to provide a sufficient level of protection of individuals’ privacy, liberties and fundamental rights with regard to European standards.\(^{37}\) There are various exemptions, including:\(^{38}\)

- if the data subject has expressly consented to the transfer;
- if the transfer is necessary for the protection of the data subject's life or the protection of the public interest;
- if the transfer is necessary to meet obligations ensuring the establishment, exercise or defence of legal claims;
- if the transfer is necessary for the legal consultation, in accordance with legal conditions, of a public register that, according to legislative and regulatory provisions, is intended for public information and is open for public consultation by any person demonstrating a legitimate interest;
- if the transfer is necessary for the performance of a contract between the data controller and the data subject, or of pre-contractual measures taken in response to the data subject’s request;
- if the transfer is necessary for the conclusion or performance of a contract, either concluded or to be concluded in the interest of the data subject between the data controller and a third party;
- if the EU's standard contractual clauses (Model Contract Clauses) are used for the transfer of personal data; and
- if the data controller has entered into binding corporate rules (BCRs).\(^{39}\)

\(^{36}\) Resolution No. 2005-51 of 30 March 2005 on review of a draft code of conduct introduced by the French Union for Direct Marketing on use of electronic contact details for direct marketing, and Resolution No. 2005-47 of 22 March 2005 on review of a draft code of ethics presented by the National Union for Direct Communication on electronic direct communications.

\(^{37}\) Article 68 of the Data Protection Law.

\(^{38}\) Article 69 of the Data Protection Law.

\(^{39}\) BCRs are internal rules developed by the Article 29 Working Party to govern international data transfers within companies or groups of companies.
V  GDPR

The CNIL has published a six-stage programme and tools to help organisations prepare for the GDPR. Compliance with the GDPR is particularly focused on the processing register and internal documentation, privacy impact assessments for risky processing and notification of violations of personal data.

Labels

The CNIL may issue certification labels to products or procedures for the protection of individuals with regard to the processing of personal data. The CNIL label is an acknowledgment by the CNIL for companies, authorities, associations or administrations that a product or procedure is compliant with the Data Protection Law. This label is issued according to a standard adopted by the CNIL and published in the Official Journal. There are currently four CNIL labels (for processing audits, training, governance and safety).

VI  COMPANY POLICIES AND PRACTICES

General obligations

The wording and updating of policies and practices is a sign of good management of personal data – taken into account by the CNIL in the event of checks or audits – provided they are in full compliance with the applicable law and take into account both technological developments and the CNIL’s evolving doctrine. It is particularly recommended that companies have:

a  a personal data protection and privacy policy;
b  a storage and archive policy;
c  a process for the management of access rights;
d  a register of personal data processing, including risk assessments;
e  notices of information specific to each situation; and
f  a code of conduct for good uses of technology resources, internet and social media usage.

VII  DISCOVERY AND DISCLOSURE

Any communication of information under discovery proceedings shall be in accordance with Article 23 of the Hague Convention of 18 March 1970 and Article 1(b) of Law No. 68-678 of 27 July 1968 (the French blocking statute).

The Data Protection Law applies, since the communication involves personal data processing and transfers of personal data outside the European Union.

As a result, dependent on circumstances, a notification or a demand of authorisation to the CNIL is necessary. Discovery procedures must meet the following principles:

a  legitimacy of processing and maintaining of professional secrecy;
b  proportionality and adequacy of data (local data filtering);
c  limited period of storage;

d  a register of personal data processing, including risk assessments;

41  Article 11.3(c) of the Data Protection Law.
42  Created by Law No. 80-538 of 16 July 1980 on disclosure of documents or information on an economic, commercial, industrial and technical matter to individuals or foreign corporations.
d security measures;
e provision of information to data subjects on their rights; and
f compliance with provisions relating to personal data transfers.

The CNIL has published recommendations regulating the e-discovery procedure.43

VIII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies
The CNIL is responsible for enforcing the Data Protection Law. For this purpose, the CNIL may:44

a receive claims, petitions and complaints relating to the carrying out of the processing of personal data, and inform the initiators of such actions of the decisions taken regarding them;
b respond to requests from public authorities and courts for an opinion, and advise individuals and bodies that set up or intend to set up automatic processing of personal data;
c immediately inform the Public Prosecutor of offences of which it has knowledge and may present its observations in criminal proceedings; and
d entrust one or several of its members or its general secretary to undertake – or have undertaken by staff members – audits and controls relating to any processing.

In the event of a breach, the Select Committee of the CNIL has the power to pronounce penalties after the due hearing of all parties,45 such as warning a data controller failing to comply with the obligations required by the Data Protection Law, financial penalties or injunctions to cease processing.

If processing or using processed data leads to violation of rights and liberties, the Select Committee may, after hearing both parties, initiate an emergency procedure to decide on suspending processing for a maximum period of three months.

During the hearing of the parties by the Select Committee, data controllers may be represented by their attorney.

ii Recent enforcement cases
Examples of recent enforcement cases by the CNIL
According to its latest annual report, the CNIL ordered 430 audits in 2016, issued 82 warnings and imposed 13 penalties.

In 2017, Facebook received a €150,000 fine46 for massively combining the personal data of internet users for the purpose of targeting advertising, and for tracking users, with or without an account, without their knowledge, on third-party sites using cookies.

43 Resolution No. 2009-474 of 23 July 2009 on recommendations for transfer of personal data within American ‘discovery’ judicial procedures.
44 Article 11 of the Data Protection Law.
45 Article 45 of the Data Protection Law.
The CNIL also imposed a €40,000 fine on car rental firm Hertz France, finding that the company had breached its data security obligations. In addition, the CNIL issued a public warning against peer-to-peer car rental company OuiCar, finding that it had breached its obligations regarding the security and confidentiality of personal data. With the facts having taken place before the entry into force of the DRA, the company only incurred a warning. A financial penalty could now be imposed in a similar case. In late 2016, the CNIL also issued a public warning against the French Socialist Party in respect of membership-request data from its website being accessible to unauthorised persons, and for failings in security procedures, which fell short of current best practices.

In this context, when performing its enforcement function the CNIL takes into account not only whether a data breach actually occurred, but also whether security measures in place (password security, encryption of data, methods of transmission, etc.) are up to the standard of current best practices.

In addition, at the end of June 2016, the CNIL decided to conclude the public notice procedure it had launched against Microsoft Corporation, finding that it had made the modifications requested in the Windows 10 operating system. This procedure, initiated a year ago, followed a series of seven online checks carried out by the CNIL between April and June 2016.

IX CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Data Protection Law applies to processing of personal data if the data controller is established on French territory. Data controllers operating within an establishment, whatever its legal form, are considered to be on French territory.

The Data Protection Law applies to the processing of personal data if the data controller – even if it is not French or situated in any other Member State of the European Union – uses a means of processing located on French territory, unless the processing is merely for the purposes of transit through this territory or that of any other Member State of the European Union.

In such cases, data controllers shall notify the CNIL of the appointment of a representative established on French territory who will represent them for the fulfilment of the duties required by the Data Protection Law.

X CYBERSECURITY AND DATA BREACHES

i Vulnerability Disclosure Policy

The DRA has created an official procedure for the disclosure of security vulnerabilities (new Article L2321-4 of the Defence Code). A person acting in good faith may inform the ANSSI – the governmental agency in charge of information security – of the existence of a security vulnerability. The ANSSI must ensure the confidentiality of the identity of its informant.
The ANSSI may then investigate the reported vulnerability by performing the technical operations strictly necessary to assess its risk or danger, and warn the person in charge of the information system at issue.

ii  Digital Safe
The DRA also defined a ‘digital-safe’ service (new Article L137 of the Post and Electronic Communication Code). Specifically, this service aims to allow the reception, conservation, deletion and transmission of electronic data and documents under conditions permitting demonstration of their integrity and their origins. The ANSSI certified the first digital-safe provider in September 2016.51

iii  Cloud computing
In December 2016, the ANSSI issued new specifications relating to the ‘essential’ level of its secured-cloud qualification programme, SecNumCloud.52 Specifications relating to an ‘advanced’ level are still being drafted at the time of writing. Three service providers are currently undergoing qualification.53

Together with its German equivalent (BSI), the ANSSI also developed a common standard, called ESCloud, based on its own SecNumCloud programme and the German one, BSI C5.54

iv  Qualified trust service providers

v  Cybersecurity of industrial control systems – vital operators
Pursuant to the French Defence Code (Article L2321-1 et seq. and Article L1332-6-1 et seq.), it is the responsibility of the state to ensure adequate security of vital operators’ critical systems. The state must:
   a  determine certain security-related obligations, such as prohibiting the use of certain systems connected to the internet;
   b  implement detection systems using providers certified by the state;
   c  systematically audit the security level of critical information systems; and
   d  impose any necessary measures on operators in the event of a major crisis.

Vital operators are required to report incidents to the relevant authorities to give advance warning to companies that could potentially be affected by the same type of attack.55

53  https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud.
55  Article L1332-6-2 of the Defence Code.
The ANSSI has also published key measures to improve the cybersecurity of industrial control systems. Various sector-specific rules were adopted in 2016 for operators of vital importance in the health, water, foodstuff, energy and transport sectors.

The current legal framework will soon be subject to an overhaul based on the transposition into French law of Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. The ANSSI will be in charge of this process, with 9 May 2018 being the final deadline for the transposition.

vi  **Interception devices**

The 2013 Military Planning Law extended the authorisation regime applicable to interception devices to products that, although not specifically designed for interception purposes, are ‘of such a nature as to enable’ the interception of communications.

The necessary enforcement measures were adopted in August 2016, and entered into force on 1 October 2016.

This will result in a significant increase in the number of products that will need to be authorised before being marketed or purchased, and will require close cooperation with the ANSSI.

vii  **Administrative access to information and data connections for the purpose of investigation**

Article L246-1 et seq. of the Homeland Security Code provide that the intelligence services of the Ministries of Defence, the Interior, the Economy and the Budget may access personal information and data connections (including location-based mobile terminals, such as smartphones, in real time) stored by electronic communications operators, ISPs and hosts for the following reasons: searching information relating to national security; safeguarding essential elements of France’s scientific and economic potential; and the prevention of terrorism, organised crime and the rebuilding or maintaining of dissolved groups.

Article L853-1 et seq. of the Homeland Security Code also allow administrative authorities to authorise the marking of vehicles or objects, the picking up of sound or images in private places and computer data capture; and by means of supervised access to the networks of telecom operators, the monitoring of individuals identified as posing a terrorist threat.

viii  **Breach of security – public electronic communication services**

Article 34 bis of the Data Protection Law provides that security breaches (any breach of security leading accidentally or unlawfully to destruction, loss, alteration, disclosure or unauthorised access to personal data processed in the context of providing electronic communication services to the public) should be immediately notified to the CNIL. The CNIL announced that a new online notification service will be available in May 2018, in accordance with the GDPR.56

56  https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser.
Only providers to the public of electronic communication services using electronic communication networks with open public access are affected by this requirement. They must establish and maintain an inventory of violations and make it available to the CNIL.

If a violation is likely to breach personal data security or the privacy of a subscriber or any other individual, the provider must also immediately notify the party affected.

ix Criminal penalties for cybersecurity attacks

The Criminal Code lays down penalties for cybersecurity offences. For example, Article 226-4-1 of the Criminal Code renders digital identity thieves liable to one year in prison and a €15,000 fine. On this basis, the French Supreme Court upheld a judgment sentencing a person to a €3,000 criminal fine for creating a website exploiting a security vulnerability in the website of a French politician to publish false press releases.57 Moreover, Article 323-1 of the Criminal Code penalises unauthorised access to a computer system with two years’ imprisonment and a fine of €30,000.

XI OUTLOOK

Governance of information systems and data is becoming a strategic concern for companies, both internally and in terms of their external dealings, as well as in relation to interactions with intermediaries when subcontracting, outsourcing, etc. Furthermore, while the size of a company will also have a bearing on these matters, both large corporations and small businesses are affected. To date, there are no mandatory requirements in France encompassing the governance issue as a whole, but various initiatives contribute to its furtherance.

One of the major trends in this regard is ‘privacy by design’, which aims to integrate personal data protection into processes from the outset, in terms of technology, internal practices and physical infrastructure. The CNIL labelling scheme also contributes to the rationalisation of data management.

Labelling (as well as certification and qualification) is also a major trend in cybersecurity, with the ANSSI providing both the technical requirements to be met and assessment services. On an international level, the ANSSI also perceives the redefinition of the rules applying to cooperation, regulation and dispute resolution as a key challenge, and it is collaborating on this with the French Foreign Office.

57 Supreme Court, Criminal Chamber, 16 November 2016, Docket No. 16-80.207.
I OVERVIEW

Germany has been and still is the forerunner on privacy and data protection law. In 1970, the German state of Hesse enacted the world’s first Data Protection Act. The other states soon followed, and on 1 January 1978, the first German Federal Data Protection Act (BDSG) entered into force. These acts established basic principles of data protection, such as the requirement of a legal permission or the data subject’s consent for any processing of personal data. In 1983, the German Federal Constitutional Court held that the individual even has a constitutional right to ‘informational self-determination’. The background of this groundbreaking verdict was a census planned for the year 1983, which essentially focused on the census of the entire German population by the means of electronic data processing. The people of Germany were anything but pleased with this idea and – as a consequence – more than 1,600 complaints were filed at the Federal Constitutional Court against the census law that had been specifically adopted for the census by the German parliament. Finally, in December 1983, the German Federal Constitutional Court declared certain provisions of the Census Act to be unconstitutional.

Over time, the German Federal Data Protection Act was subsequently amended and now contains separate provisions for data processing in the public and private sectors. In addition, Germany has specific privacy provisions for electronic information and communication services (the Telemedia Act of 2007 (TMA)) and yet another set of privacy rules for the providers of services that transmit electronic signals (the Telecommunications Act). Through these different laws, Germany transposed the European Union (EU) Directives 95/46/EC and 2002/58/EC, albeit in a very complex and differentiated manner.

In keeping with the EU Directives, Germany generally prohibits the collection and use of personal data unless the law specifically permits this or the data subject has given his or her informed consent. German law also follows the Directives on issues relating to rights and remedies of data subjects, security requirements, restrictions on location data, minimisation of data and safeguards against transmitting personal data to third countries with lesser standards of protection. The provisions, however, often call for the balancing of competing interests – especially the right of free speech, as well as the public’s right to know and the application of the principle of proportionality. As a consequence, these provisions...
have resulted in extensive and varied case law. As this book focuses mainly on aspects of cybersecurity law, the authors of this chapter will often refer to online-related cases and laws. This does not mean, however, that the same principles do not apply to ‘offline’ cases as well.

The following text provides an overview of the current legal situation in Germany and an outlook of the changes that are poised to come into force in May 2018.

II THE YEAR IN REVIEW

The past year was marked by the upcoming adoption of Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), which will eventually replace the German data protection laws to a large extent in 2018.

As a regulation, the new framework does not have to be transposed into the different national laws of the European countries but will be directly applicable in all EU Member States. However, as a specialty of the GDPR, the regulation also contains ‘opening clauses’ that provide Member States with the discretion to introduce additional national provisions to concretise and further specify the application of the GDPR for specific issues (e.g., in connection with employees). To that end the German parliament passed a new version of the BDSG in April 2017. This new set of rules, the GDPR and the new German BDSG, will come into force in May 2018.

It will be particularly interesting to see how the new rules will affect smaller businesses as well as international companies – especially in the way they organise their internal compliance management systems. Although the GDPR will maintain the main concepts of data protection as we know them today to a large extent, or amend them just in detail (e.g., data processing is still prohibited if not explicitly permitted by the data subject or a law, the legal bases for the transfer of personal data into non-EU countries or the obligation to designate a data protection officer), the new rules also bring some important changes.

First and foremost, the GDPR extends its territorial scope, which means that non-European companies may also fall within its scope, making it the first worldwide data protection law. It applies to (1) all companies worldwide that target European markets and in this context process personal data of European Union citizens (irrespective of where the processing takes place) and (2) those that process data of European citizens in the context of their European establishments. The GDPR tightens the rules for obtaining valid consent to process personal information. Valid consent is one of the two possibilities to justify data processing, with the other being legal justification. Companies will therefore have to update their consent management.

Further, the GDPR extends the documentation obligations for companies and changes the burden of proof. As a consequence, companies will have to prove that they fulfil their obligations under the GDPR to the data protection offices.

The GDPR also introduces mandatory privacy impact assessments (PIAs). It requires data controllers to conduct PIAs where privacy breach risks are high to minimise risks to data subjects. This means that before organisations can begin projects involving personal data, they will have to conduct a PIA and work with the data protection offices to ensure they are in compliance with data protection laws as projects progress.

The GDPR also contains a data breach notification requirement. It harmonises the various data breach notification laws in Europe and is aimed at ensuring that organisations constantly monitor potential breaches of personal data. The regulation requires organisations to generally notify the local data protection authority of a data breach within 72 hours of
discovering it. This means organisations need to ensure they have the technologies and processes in place that will enable them to detect and respond to a data breach in time. For many organisations, this could require quite a bit of training. It may also require making changes to internal data security policies and how these are promoted in the organisation to ensure necessary procedures are properly understood and will be followed easily.

The GDPR expands liability beyond the data controllers. In the past, only data controllers were considered responsible for data processing activities, but the GDPR extends liability to all organisations that process personal data. The GDPR also covers any organisation that provides data processing services to the data controller, which means that even organisations that are purely service providers that work with personal data will need to comply with rules such as data minimisation.

The enforcement of the GDPR is backed by significant fines of up to €20 million or 4 per cent of annual global turnover, whichever is higher.

The GDPR is, as a regulation, directly applicable as of 25 May 2018 – without any grace period.

III REGULATORY FRAMEWORK UNTIL MAY 2018

Privacy and data protection legislation and standards

Although there will be some major changes to the current regulatory framework from 25 May 2018 onwards, at present and for the months prior to this date the BDSG remains fully applicable.

The BDSG currently defines personal data as ‘individual pieces of information about personal or factual circumstances about an identified or identifiable human being’. This definition applies to all personal data handled by electronic information and communication (telemedia) service providers irrespective of whether the data are governed by the BDSG or the TMA. Different rules on consent requirements, however, apply to different categories of data.

Contract data, as defined by the TMA, are the data required to establish, develop or change a contractual relationship with a telemedia service provider. Contract data are to be collected sparingly, to satisfy the principle of data minimisation. They may only be used for the intended contractual purpose and must be deleted once they are no longer needed. This use is statutorily permitted. The data subject’s specific consent, however, is required if the service provider intends to use the data for other purposes, such as advertising or market research. The provisions on contract data apply whenever a relationship is established by an online registration. They apply therefore, for example, to Facebook and other social media.

Utilisation data are the personal data that a telemedia service provider may collect and use to facilitate use of the service and for accounting purposes. The service provider may use these data to create user profiles for market research and advertising, unless the user objects after having been duly informed. The thus created profiles must be identified by a pseudonym, and the identity of the user may not be revealed.

Other data, particularly content data, fall under the consent requirements of Sections 28 to 30 BDSG if they are collected by online service providers. In their current form, these provisions were introduced through the 2009 reform of the BDSG, and their complexity is legendary. Generally, they allow certain commercial uses of data, including ‘list-making’ and ‘scoring’, albeit under numerous safeguards. Section 29 deals with commercial data collection
and storage for the purpose of transferring the data to third parties, including for marketing. Such activities are permitted to some extent without the data subject’s consent, but the competing interests must be balanced.

There has been much discussion of whether IP addresses are personal data. With its judgment of 16 May 2017, the Federal Supreme Court (BGH) has decided that dynamic IP addresses are generally personal data. At the same time, the BGH dealt with the question of the circumstances under which IP addresses may be stored by website operators. It has been decided that storage is allowed if there is the risk that the website may be attacked by hackers. As far as it is clear that the storage is necessary for the functionality of the website, a second step should be to examine whether, in the specific case, the operator’s security interest prevails over the user’s right of personality. The greater the risk of an attack, the more likely it becomes that the storage of personal data is lawful. In any event, a decision must always follow a case-by-case assessment.

The BDSG defines ‘sensitive data’ according to Directive 95/46/EC as that data relating to race, ethnicity, political opinions, religious or philosophical beliefs, or health or sex life. Consent must be expressed specifically in connection to such sensitive data to permit the collection and use of the data.

ii General obligations for data handlers
The privacy provisions of the BDSG address data controllers, namely entities that process personal data on their own behalf or commission others to do the same. Telemedia service providers as data collectors may collect and use personal data only to the extent that the law specifically permits, or if the data subject has given his or her consent. Moreover, to the extent that the law permits the collection of data for specified purposes, these data may not be used for other purposes, unless the data subject has consented to other uses.

According to Section 13 TMA, the controller must inform the user of the extent and purpose of the processing of personal data for any consent to be valid. Consent may be given electronically, provided the data controller ensures that the user of the service declares his or her consent knowingly and unambiguously, the consent is recorded, the user may view his or her consent declaration at any time and the user may revoke consent at any time with effect for the future. These principles accord with Section 4a BDSG, which requires consent to be based on the voluntary decision of the data subject. Consent, however, is not always required. Many statutory exceptions allow for the use of data without consent, for various business-related purposes.

According to Section 13 Paragraph 1 TMA, a telemedia service provider must inform the user at the beginning of the contractual relationship of the extent and purpose of data collection and use, and whether the data will be processed outside the European Union. If the provider intends to use an automated process that will allow the identification of the user, then this information has to be provided when data collection commences, and the user must at any time have access to this instruction.

This provision of the TMA has been interpreted as applying only to contract and usage data, thus leaving content data under the governance of Section 4 Paragraph 3 BDSG. The latter provides that the controller must inform the data subject of the identity of the data controller, the purpose of the collection, processing and use of the data, and the categories of intended recipients if this is not foreseeable for the data subject. This information must be provided when the data are first collected.
In addition to necessary imprint information, any service provider that collects, processes or uses personal data on a website is, therefore, obliged to publish a privacy policy on his or her website. The information provided in the privacy policy has to meet the requirements of Section 13 TMA. This means that the information has to be provided at the beginning of the session, and in a generally comprehensible and understandable manner. In addition, it needs to be accessible by the recipients at any given time.

The question of when a given act of processing must be notified to the supervisory authority depends on the act of processing itself and the structure of the responsible entity wishing to carry out the processing. This differentiation sets Germany apart from many of the EU Member States that require every act of processing to be formally notified to the supervisory authority before they can be implemented. However, with the exception of small corporations and insignificant acts of processing, the fact that there do exist certain carve-outs should not be taken to mean that the supervisory authorities will not take notification duties seriously; they have the right to audit responsible entities regardless of whether these have notified them of any act of processing.

Section 4d Paragraph 1 BDSG establishes an obligation for private entities to notify the competent authority if any data are processed by automated means, as well as setting out exceptions to that requirement. The duty to actively notify acts of processing to the supervisory authority does not exist where the responsible entity has appointed a data protection officer in accordance with Section 4f and 4g BDSG, or if the entity concerned deals with personal data for its own purposes and employs no more than nine people permanently in the automated processing of personal data. These exceptions do not apply, however, if the personal data are gathered to transfer it or to use it for market research.

iii Technological innovation and privacy law

Cookies

Under German data protection law, the use of cookies is only relevant if the information stored in the cookie is considered personal data. A cookie is a piece of text stored on a user’s computer by his or her web browser. A cookie may be used for authentication, storing site preferences, the identifier for a server-based session, shopping cart contents or anything else that may be accomplished through the storage of text data. The cookie is considered to be personal data if and when it contains data that allow the controller to identify the data subject. This might also be the case when the data subject cannot be identified by the cookie data itself, but only by means of other data that can be accessed by the controller and linked to the data contained in the cookie. In such an event, the use of the cookie is only considered to be lawful if it is validated by the data subject’s consent. It has been controversially discussed whether the consent must be given via an opt-in or an opt-out method. The former method would require a site operator to ask for consent before any cookie is placed in the user’s browser. The second method allows the placement of cookies until the user actively withdraws his or her consent. Section 5 Paragraph 3 of the ‘ePrivacy Directive’ states that prior consent has to be given by the user. However, in Germany, no additional legislation was passed after the ePrivacy Directive came into force. Instead, the German legislator is of the opinion that the existing Section 15 Paragraph 3 TMA already addresses this issue appropriately. This Section allows the use of cookies as long as the user does not object. In 2014, the EU Commission confirmed that the TMA successfully implements the ePrivacy Directive into national law. For the time being, cookies may be placed in Germany as long as the user has the option to object (opt out). With respect to website providers offering services that
require an application, the consent for the use and processing of cookies containing personal data may be obtained during the application process. The use of cookies for the purposes of advertising, market research or to organise telemedia on the basis of need is lawful without consent to the extent permitted by Section 15 Paragraph 3 TMA.

**Cloud computing**

Cloud computing raises difficult data protection issues. Cloud computing relationships are technically complex and often involve the transfer of data across multiple jurisdictions, as the physical location of data in the cloud is often not bound to a specific server in a specific country. Moreover, it is virtually impossible, at least for the data subject, to know for certain whether all servers used are effectively secure, or to determine who has control over and insight into the data. The reason for this is the assumption that there is generally no adequate data protection level in third countries. Accordingly, data transfers to non-EU countries will continue to be permitted only if additional security mechanisms help to ensure an adequate level of data protection, or such an adequate level is bindingly identified by the European Commission. The controller must ensure that his or her use of the cloud computing services is in compliance with the requirements outlined in Section 4b Paragraph 2 BDSG, with respect to cross-border data transfer, processing and use. This is a highly complicated task. For instance, the controller will have to ensure that the cloud service provider observes an adequate data protection level at all times.

**Social media**

The role of social media in the recruitment process of employers is subject to intense scrutiny by lawmakers and supervisory authorities as some statistics suggest that over 46 per cent of employers try to gain valuable information about their applicants through social media platforms.

As a result, there is a perceived need to protect potential and current employees, especially younger employees just starting a career, from the adverse effects of publications they may have made about themselves and later regret. Under the current Section 32 BDSG and the proposed and identical Section 26 of the new BDSG, an employer may search social media sites for information that is necessary for recruitment purposes or the current employment. Therefore, inquiries about personal data are illegal under German law, but searching social media sites or the internet in general for business-related information regarding a prospective new employee might be allowed as long as the data collection is limited to the candidate’s professional knowledge, skills and experience with regard to the position to be filled.

As far as the collection of data is not permitted by Section 32 BDSG, Section 28 BDSG may also provide a legal justification. To this end, the data concerned would have to be generally accessible and the applicant’s legitimate interest in the exclusion of processing or use would obviously not prevail over the legitimate interests of the employer company. One argument to decide on the legality of the data collection may be provided by the purpose of the particular social network. For business-oriented social networks, such as LinkedIn, data collection might be legally permissible. By participating in the network, the applicant would like to expand and cultivate his or her professional contacts and to present himself or herself as a professional, and also present his or her professional experience. In the case of often exclusively privately used social networks, such as Facebook, the applicant’s legitimate interest should be predominant and the collection of data should be inadmissible.
iv Sharing employee data in groups of companies

Perhaps the most common cause for centralised collection, processing or use of personal data in an employment relationship, is the use of tools and IT infrastructure shared across multiple legal entities in groups of companies, and the use of shared services and shared functions, whereby individual centralised organisations take the place of hitherto decentralised staff functions. A good example is provided by employee self-service help desks and centralised human resources departments supporting any number of legal entities in multiple countries and interfacing directly with the employees and their managerial structure.

The use of personal data in an employment relationship is associated with particular compliance requirements when the use is to be carried out by another legal entity within a group of companies that is not the legal employer of a given employee. The underlying reason for these issues is that Section 32 Paragraph 1 Sentence 1 BDSG includes a justification for processing personal data where it is required to fulfil an employment relationship. This justification, however, is limited to the employment relation between the employer and the employee only, and only the legal entity actually holding the employment contract, the ‘legal employer’, can draw upon the justification. Other legal entities in a group of companies that the legal employer is also a part of cannot rely on this justification, even though the employee may be interfacing with employees of the group members on a fairly regular basis.

This absence of a group privilege or – to phrase it differently – the fact that the law does not recognise an intra-group exemption to transfer data freely between group companies is a major barrier to the free interchange of personal data in groups of companies. In effect, it causes each single legal entity in a group of companies to be considered separately, and any intra-group transfer of data regarding an employee is treated just as if the other legal entity were not part of the group of companies at all. It is necessary to visualise this issue to appreciate the fact that centralised functions in a group of companies cannot generally rely upon the justification that their use of personal data satisfies the requirements of the fulfilment of the employment contract. To overcome this obstacle, a viable option for corporations can be the establishment of central processing structures of personal data in groups of companies by utilising the concept of commissioned data processing according to Section 11 BDSG.

If a legally independent company is acting as a commissioned data processor pursuant to Section 11 BDSG for one or more other group companies, the contracting entities are not ‘third parties’ in relation to each other and the transfer of data between them does not constitute a ‘transmission’ within the meaning of Section 3 Paragraph 8 Sentence 3 BDSG and Section 3 Paragraph 4 No. 3 BDSG.

According to the working group, the transmission of employee data can be justified under Section 28 Paragraph 1 No. 1 BDSG when the employment contract expressly allows the employee to work for other corporations in the group. This is especially the case for high-level executive employees whose duties are related not just to their legal employers, but also to the group and who are aware of the mobility between corporations necessary to fulfil their employment contract.

IV INTERNATIONAL DATA TRANSFER

The international transfer of personal data is regulated within the framework of Sections 4b and 4c BDSG. There is a general distinction between transfers within the EU and EEA or to one of the ‘trusted countries’ for which the European Commission has confirmed by means of an ‘appropriateness decision’ that these countries ensure an adequate level of data
protection on the one hand and transfers to third countries on the other. For an international data transfer to be lawful, it must comply not only with Sections 4b and 4c BDSG, but must also be in compliance with the general provisions pertaining to the legality of processing operations involving personal data.

i Data transfer within the EU or EEA

Section 4b BDSG states that international transfers of personal data within the area of the EU or EEA are covered by the same rules as national data transfers within Germany. For these international data transfers, private entities merely require a legal permission under Sections 28 to 32 BDSG, or the data subject’s consent.

ii Data transfer to countries outside the EU or EEA

If a private entity intends to transfer personal data internationally to another entity located outside the area of the EU or EEA (a third country), Section 4b Paragraph 2 Sentence 2 BDSG stipulates additional requirements. In this respect, personal data shall not be transferred when the data subject has a legitimate interest in being excluded from the transfer. A legitimate interest is assumed when an adequate level of data protection cannot be guaranteed in the country to which the data are transferred.

An adequate level of data protection exists in certain third countries that have been identified by the European Commission. These are Andorra, Argentina, Guernsey, the Isle of Man, Canada (limited), Faroe Islands, Israel (limited), Guernsey, Jersey, New Zealand, Switzerland and Uruguay. Any transfer of personal data to these countries will only have to satisfy the requirements of data transfers within the EU or EEA.

Uncertainty currently surrounds data transfers to the United States. After the European Court of Justice declared the Safe Harbor principles of the Commission invalid, the Commission enacted the EU–US Privacy Shield. Under the protection of the new principles of the Privacy Shield the United States is found to have an adequate level of data protection. But the Privacy Shield itself is again the target of a great deal of criticism. There are currently several complaints pending against the Privacy Shield at the European Court of Justice.

Data transfers to any other non-EU country may be justified by the derogation rules of Sections 4b and 4c BDSG. Under Section 4c Paragraph 1 BDSG, the international transfer of personal data is admissible if:

a the data subject has given his or her consent;

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 in response to the data subject’s request;

c the transfer is necessary for the conclusion or performance of a contract that has been or is to be concluded in the interest of the data subject between the controller and a third party;

d the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

e the transfer is necessary to protect the vital interests of the data subject; or

f the transfer is made from a register that is intended to provide information to the public, and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law are fulfilled in the particular case.
The most relevant grounds are those given at (b), namely if the transfer is necessary to perform a contract between the data subject and the controller. This includes international monetary transactions and distance-selling contracts as well as employment contracts. All transfers in this respect have to be essential for the purposes of the contract.

Any consent within the meaning of (a) will only be valid if the data subject was informed about the risks that are involved in data transfers to countries that do not have an adequate standard of data protection. In addition, the consent has to be based on the data subject's free will; this may be difficult if employee data are involved.

If none of the aforementioned exceptions applies, the transfer of personal data to third countries with an inadequate level of data protection is nonetheless possible if the competent supervisory authority authorises the transfer. Such an authorisation will only be granted when the companies involved adduce adequate safeguarding measures to compensate for a generally inadequate standard of data protection: see Section 4c Paragraph 2 BDSG. The primary safeguarding measures are the use of standard contractual clauses issued by the European Commission and the establishment of binding corporate rules.

V DISCOVERY AND DISCLOSURE

The 2009 amendments to the BDSG require companies to report an abuse or loss of certain sensitive data to the relevant German supervising authority as well as to the affected persons. The amendments also increased fines for serious data privacy breaches to €300,000. In 2011, the German data protection authority issued a set of guidelines explaining the data-breach provisions of the amendments. In contrast to US discovery rules, German law generally does not require litigants to disclose documents to the other party. German authorities will nevertheless permit very limited discovery for pending US proceedings if the US court sends a letter of request for specific documents needed to resolve an issue.

Discovery of workplace emails in Germany is particularly challenging. The BDSG limits the use of nearly all employee personal data, which is defined to include most employee emails. If an employer permits employees to use their computers at work for private communication, then those communications are likely to be protected from discovery. The distinction between private and employment-related communication is sometimes difficult to make, and it is unclear how much of an employee's email would ultimately be excluded from discovery for privacy reasons.

Germany has at least one blocking statute, the Federal Maritime Shipping Act of 24 May 1965, which was enacted to frustrate attempts by the United States Federal Maritime Commission to gather information from shipping lines concerning allegations of anticompetitive practices.

VI PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Germany has a Federal Data Protection Agency and 16 state data protection agencies. These often act in concert when making recommendations on how the consumer may navigate safely through the internet. In addition, German experts often discuss the data protection problems that arise from the widespread collection of data by search engines and social media, and the use of these data to profile the data subject for commercial purposes. Although
German law prohibits these practices unless informed consent has been given, and although German law applies to any collection of data on German soil, Germany cannot yet enforce these laws against global actors.

The Federal Data Protection Agency is charged with supervising the data privacy compliance of federal entities and certain non-public entities, such as telecommunications service providers that are subject to specific supervision, as well as the application of the German Freedom of Information Act as of 1 January 2006.

The state data protection agencies are charged with supervising the data privacy compliance of state entities, as well as all non-public entities whose principal place of business is established in the state and that are not subject to the exclusive jurisdiction of the federal supervisory authority. In states that have enacted a freedom of information act, the state supervisory authorities are typically also charged with supervising the act’s application by state entities.

The heads of the supervisory authorities are typically appointed by the federal and state parliaments respectively, and are required to report to their respective parliaments.

ii Material enforcement cases

Sections 43 and 44 BDSG regarding administrative and criminal offences have been substantially enlarged by the most recent redraft of the BDSG, which entered into force in 2009. It was introduced by the government as a consequence of a series of data protection scandals involving prominent German companies. Penalties were increased to €50,000 for failure to comply with formalities and €300,000 for other data protection breaches. Most of these data protection breaches were caused by internal compliance activities of companies where the responsible management carelessly contravened the high standards of German data protection law (e.g., through video surveillance or screening bank account details). The main reason for wrongdoing was the false understanding that compliance activity by its nature is a justification for any use of personal data. This assumption turned out to be incorrect.

For instance, in October 2009 the Data Protection Authority of Berlin imposed a fine of €1.124 million on Deutsche Bahn AG for significant violations of the data protection law. This is allegedly the highest administrative fine ever imposed in Germany for non-compliance with the data protection law. Deutsche Bahn AG was fined for mass screenings of employee data, including names, addresses, telephone numbers and bank details, and for matching them with supplier data, supposedly to detect fraudulent activities, in particular employee-fronted shell companies.

In fact, there is no statutory law justifying the use of personal data for compliance activities on a general level. This has to be decided on a case-by-case basis. Consequently, depending on the circumstances of the actual matter, the disclosure of personal data without the consent of the data subject or the explicit statutory right to do so may be subject to punishment according to Sections 43 and 44 BDSG, with sanctions of imprisonment for up to two years or a fine.

iii Private litigation

The privacy rights and remedies of telemedia users are governed to a large extent by the BDSG. The BDSG imposes duties of notification on the data controller (see Section 4, Paragraphs 3 and 33 BDSG). He or she must notify the data subject of the types of data that are being collected, the source of the data, the purposes for which the data are collected and to whom they are disclosed.
For the data subject, Section 34 BDSG grants rights of access and rights to effect correction, erasure and blockage (Section 35 BDSG). The right to demand erasure often becomes an issue when a user leaves a social networking medium. Users often waive the right of erasure in the standardised terms of contracts. It appears that this is currently permissible according to German law. Even if erasure were to be carried out, data are transmitted to third parties in many different ways in social media, so that erasure often does not fulfil its purpose.

Data subjects may enforce their rights through the judicial remedies provided in civil law. Injunctive relief as well as damages can be claimed. However, damages for pain and suffering are not available for data protection violations under civil law.

In Germany, the data protection authorities are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers must first be lodged with the company’s in-house data protection officer (see Section IX.ii).

VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

In keeping with Article 4 of Directive 95/46/EC according to Section 1 BDSG, the law of the seat of the controller applies to data processing occurring in Germany if the controller resides in another Member State of the European Union. German law applies, however, if that EU-resident controller carries out data processing in Germany through a German subsidiary or establishment. German law also applies for any data processing occurring in Germany that is carried out by a controller who resides outside the European Union.

According to these principles, German law applies to an online search engine or social medium if it places a cookie on a German personal computer. Enforcement of German law, however, can rarely be achieved against foreign controllers.

The issue of the application of German law to the collection of German data by controllers in third countries is addressed in the ongoing controversy over whether Facebook qualifies as an EU-domiciled controller because of its corporate address in Ireland. Many German experts are of the opinion that the usage of Facebook in Germany, in particular the use of the ‘like’ button, is subject to German law. A German court ruled in 2016 that the implementation of the like button violates Section 13 TMG since the button transfers personal data to Facebook without obtaining the user’s consent first. The court ruled that not only Facebook but also the site operator is to be seen as a controller since the operator makes it possible for Facebook to gather the data. The appellate court asked the European Court of Justice for a preliminary ruling about this legal question. The court also asked the European Court of Justice if the site operator has to gather individual consent from the user or if the consent given to Facebook is sufficient. The ruling of the European Court of Justice is still pending.

VIII CYBERSECURITY AND DATA BREACHES

Section 9 BDSG requires extensive technical organisational measures to ensure the overall integrity of IT systems that are being used for the processing of personal data, and these requirements live up to Article 17 of Directive 95/46/EC. The German provisions, as well as the Directive, call for a proportional interpretation of security requirements by tailoring the need for security to the risk inherent in specific operations. Additional provisions on technical security are contained in Sections 107 and 109 Telecommunications Act.
Section 13 TMA requires controllers to install the necessary technical and organisational measures to ensure that:

a. the user may terminate the relationship at any time;
b. data will be automatically erased or blocked if required by law;
c. the use of the service will not become known to third parties;
d. data on the use of several telemedia by one user can be accessed separately, although they can be combined for accounting purposes; and
e. data collected under a pseudonym cannot be combined with data personally identifying the user.

In August 2009, Germany introduced a security breach notification requirement that obliges controllers to notify the data subject if data were unlawfully transmitted or otherwise became known to third parties. This requirement was modelled after US law and is intended to increase consumer confidence in automated systems.

Anonymising data is a general principle of German data protection law to be employed whenever feasible so as to minimise the proliferation of personal data. Data may also be placed under a pseudonym so as to preserve anonymity. These devices allow the data subject to retain control over his or her data while giving the controller greater possibilities for use and transmittal of the data. When data have been anonymised, they are no longer personal data and can therefore be freely used for market research. They become personal data again if the controller has the capacity to identify the data subject from that data. It appears that services are available in Germany that facilitate anonymity by allowing the user to communicate over an IP address that differs from his or her own.

Telemedia service providers are required to use pseudonyms for the collection of certain data. For example, for data concerning usage, the controller must employ pseudonyms to be allowed to create profiles for the purposes of market research. With regard to contract data, the telemedia service provider must make it possible for the data subject to use the service and pay for it under a pseudonym, and he or she must also inform the data subject of this option. The law provides, however, that the provider must make the use of pseudonyms possible only to the extent that it is technically feasible and can be reasonably expected. This is one of the many ‘balancing and weighing’ clauses that exist in German data protection law.

IX COMPANY POLICIES AND PRACTICES

i Compliance

Compliance with German data protection law will often require a number of agreements with different parties. In many instances, larger companies with an international approach or a German subsidiary will encounter the need for an agreement with, for instance, the data subject for collecting his or her consent or with third parties to ensure a particular level of data protection and security. Therefore, it may be useful for medium-sized or larger companies, as well as NGOs or other international practising entities, to have agreements, forms and directives adjusted to the particular situation but easily adaptable for use with different clients, customers or situations. As far as external data protection and IT security is concerned, these agreements include those concerning data protection with third parties, as well as collection, processing or use of personal data on behalf of others, IT security with third parties, granting a right to a data protection audit or disclosure agreements with third parties. As far as internal data protection and IT security is concerned, agreements might
encompass the appointment of internal or external data protection officers, data secrecy with employees, internal overview according to Section 4e BDSG, or deletion and disclosure agreements with employees.

ii  Data protection officer (DPO)

Section 4f Paragraph 1 BDSG sets forth a number of instances where private entities are obliged to appoint a DPO. According to this provision, certain medium-sized and bigger companies have to appoint a DPO. In particular, these are private entities dealing with personal data by automated means and, as a rule, employing more than nine people permanently in the automated processing of personal data. The same applies to private entities dealing with personal data by other means, and, as a rule, employing at least 20 persons for this purpose, as well as private entities carrying out automated processing of personal data in terms of Section 4f Paragraph 1 Sentence 6 BDSG.

The DPO shall ensure compliance with the BDSG and other data protection provisions. His or her general duties are described in Section 4g BDSG. Even if an entity is not obliged to appoint a DPO, it may be advisable to do so voluntarily because in that case the obligation to notify no longer applies. The German DPO is considered an important compliance function embedded in the organisation of public and private entities and – in some way – a surrogate supervisory authority and a figure of particular trust to guarantee data privacy compliance in a given entity. The person who shall be appointed as a DPO must satisfy certain requirements set forth in Section 4f Paragraphs 2 to 5 BDSG.

X  OUTLOOK

Not only in Germany, but in the whole European Union, the GDPR will standardise several aspects of privacy and data protection law. The GDPR also introduces the German concept of the DPO across the whole European Union. Naturally, companies in Germany will find it easier to comply with the new regulation than their competitors in countries that do not yet have the institution of a DPO. With the new BDSG supplementing the GDPR, May 2018 will bring a new paradigm of privacy and data protection law to Germany. It will also be interesting to see how the new statutes will be interpreted by the German and European authorities and courts.
Chapter 12

HONG KONG

Yuet Ming Tham1

I  OVERVIEW

The Personal Data (Privacy) Ordinance (PDPO) establishes Hong Kong's data protection and privacy legal framework. All organisations that collect, hold, process or use personal data (data users) must comply with the PDPO, and in particular the six data protection principles (DPPs) in Schedule 1 of the PDPO, which are the foundation upon which the PDPO is based. The Office of the Privacy Commissioner for Personal Data (PCPD), an independent statutory body, was established to oversee the enforcement of the PDPO.

Hong Kong was the first Asian jurisdiction to enact comprehensive personal data privacy legislation and to establish an independent privacy regulator. Unlike the law in several other jurisdictions in the region, the law in Hong Kong covers both the private and public sectors. Hong Kong issued significant new amendments to the PDPO in 2012 with a key focus on direct marketing regulation and enforcement with respect to the use of personal data.

Despite Hong Kong's pioneering role in data privacy legislation, the PCPD's level of activity with respect to regulatory guidance and enforcement has been relatively flat in the past year. In addition, Hong Kong has not introduced stand-alone cybercrime or cybersecurity legislation as other Asian countries have done. Certain sectoral agencies, notably Hong Kong's Securities and Futures Commission (SFC), have continued to press forward on cybersecurity regulation for specific industries.

This chapter discusses recent data privacy and cybersecurity developments in Hong Kong from September 2016 to August 2017. It will also discuss the current data privacy regulatory framework in Hong Kong, and in particular the six DPPs and their implications for organisations, as well as specific data privacy issues such as direct marketing, issues relating to technological innovation, international data transfer, cybersecurity and data breaches.

II  THE YEAR IN REVIEW

i  Personal data privacy and security developments

From mid-2015 to mid-2016, the PCPD issued a number of guidance notes, guidelines and codes of practice to assist organisations in implementing PDPO provisions. Notable publications included the October 2015 Guidance on Data Breach Handling and the Giving of Breach Notifications,2 the April 2016 Revised Code of Practice on Human Resource

---

1 Yuet Ming Tham is a partner at Sidley Austin LLP.
Management,³ the April 2016 Privacy Guidelines: Monitoring and Personal Data Privacy at Work⁴ and the June 2016 guidance note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users.⁵ None of these publications are legally binding, although failure to follow the codes of practice may give rise to negative presumptions in any enforcement proceedings.

From mid-2016 to mid-2017, the PCPD has not issued any additional codes of practice or guidelines. The PCPD has released three new revisions to existing guidance notes:

a. Guidance on Data Breach Handling and the Giving of Breach Notifications (revised December 2016) (providing assistance to data users in handling breaches and mitigating loss and damage);⁶

b. Guidance on CCTV Surveillance and Use of Drones (revised March 2017) (setting out recommendations on whether and how to use CCTV to properly protect data privacy),⁷ and

c. Proper Handling of Data Correction Request by Data Users (revised May 2017) (providing a step-by-step approach on the proper handling of a data correction request under the PDPO).⁸

The PCPD reported that it had received 1,838 complaints in 2016, a 7 per cent decrease compared to 2015.⁹ Most of the complaints involved were made against private sector organisations, with financial and property management companies leading the way. Nearly half of the complaints related to use of personal data without consent with about a third complaining about the purpose and manner of the data collection. The PCPD received 229 ICT-related privacy complaints in 2016, representing a 5 per cent decrease as compared to 2015. Most of these complaints related to the use of mobile apps and social networking websites. The PCPD received notice of 89 data breach incidents affecting 104,000 persons in 2016 compared to 98 incidents involving 871,000 individuals the year before. Direct marketing complaints increased slightly in 2016, rising from 322 to 393 cases.

With respect to enforcement in 2016, the PCPD issued 36 warnings and six enforcement notices as compared to 17 warnings and 67 enforcement notices in 2015. The PCPD sharply increased its referrals to the police of cases for criminal prosecutions in 2016 (112 compared to 30 in 2015), almost all of which involved direct marketing violations. However, the number of actual prosecutions remained relatively small (five prosecutions in 2016 compared to six in 2015). There were three convictions for direct marketing violations in 2016, two of which resulted in financial penalties.

The PCPD does not systematically publish decisions or reports based on the outcome of its investigations. For the entirety of 2016 and up until September 2017, the PCPD

---

⁶ www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf (The publication on the PCPD website has not yet been updated).
published one case note, in 2016 (finding a violation of DPP3 by a management company that had obtained personal data on one of its residents without his consent), and one investigation report, in 2017. The PCPD's 12 June 2017 investigation report related to the highly publicised loss by Hong Kong's Registration and Electoral Office (REO) of two laptops containing personal information of 3.7 million voters during the election of Hong Kong's chief executive in March 2017. The PCPD concluded that REO had breached DPP 4 (requiring the safeguarding of personal data from unauthorised access, use, or loss) and issued an Enforcement Notice against REO. Under the Enforcement Notice, the PCPD instructed REO to establish effective internal guidelines in respect of processing personal data and to ensure staff compliance with the guidelines. The PCPD also set out a number of recommendations for REO.

The PCPD made no finding of an offence committed by REO. As described below, a violation of a DPP is not itself an offence, it is only a violation of the ensuing enforcement notice that constitutes an offence. Failure to comply with the enforcement notice is an offence punishable by a maximum fine of HK$50,000 and a two-year prison term.

ii Cybercrime and cybersecurity developments

Hong Kong does not have (and as of this writing, there do not appear to be plans to establish) stand-alone cybercrime and cybersecurity legislation. The Hong Kong Police Department maintains a resource page for ‘Cyber Security and Technology Crime’, including a compendium of relevant legislation on computer crimes. These specific provisions relate to the Crimes Ordinance, the Telecommunications Ordinance and laws related to obscenity and child pornography. The government has also established an Information Security (InfoSec) website that sets out various computer crime provisions contained in the Telecommunications Ordinance, the Theft Ordinance and the Crimes Ordinance. According to the Hong Kong police, there were 5,939 computer crime cases in 2016, with an associated loss of HK$2.3 billion as compared to 6,862 cases in 2015 amounting to a loss of HK$1.8 billion.

Sectoral regulators have continued to press forward with specific cybersecurity regulation, particularly financial regulators. Both the SFC and the Hong Kong Monetary Authority (HKMA) have issued circulars on cybersecurity risk, and in May 2017, the SFC issued its Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading, as well as a circular alert on ransomware threats in the securities industry. In December 2016, the HKMA announced implementation details of its Cybersecurity Fortification Initiative undertaken in collaboration with the banking industry as well as launching an industry-wide Enhanced Competency Framework on Cybersecurity.

---

iii 2017 developments and regulatory compliance
From a regulatory perspective, the key compliance framework for companies and organisations remains with data protection and privacy. The government has not taken any additional legislative steps in the cybercrime and cybersecurity arenas although cybersecurity remains a significant challenge in Hong Kong. Financial sector regulators continue to be active with respect to cybersecurity, with the HKMA putting forward ambitious initiatives. For companies outside the financial sector, their focus will remain with PDPO compliance, particularly with the stringent direct marketing requirements.

III PDPO REGULATORY FRAMEWORK

i The PDPO and the six DPPs
The PDPO entered into force on 20 December 1996 and was amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance). The majority of the provisions of the Amendment Ordinance entered into force on 1 October 2012 and the provisions relating to direct marketing and legal assistance entered into force on 1 April 2013.

The PCPD has issued various codes of practice and guidelines to provide organisations with practical guidance to comply with the provisions of the PDPO. Although the codes of practice and guidelines are only issued as examples of best practice and organisations are not obliged to follow them, in deciding whether an organisation is in breach of the PDPO, the Privacy Commissioner will take into account various factors, including whether the organisation has complied with the codes of practice and guidelines published by the PCPD. In particular, failure to abide by certain mandatory provisions of the codes of practice will weigh unfavourably against the organisation concerned in any case that comes before the Privacy Commissioner. In addition, a court is entitled to take that fact into account when deciding whether there has been a contravention of the PDPO.

As mentioned above, the six DPPs of the PDPO set out the basic requirements with which data users must comply in the handling of personal data. Most of the enforcement notices served by the PCPD relate to contraventions of the six DPPs. Although a contravention of the DPPs does not constitute an offence, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

DPP1 – purpose and manner of collection of personal data
Principle
DPP1 provides that personal data shall only be collected if it is necessary for a lawful purpose directly related to the function or activity of the data user. Further, the data collected must be adequate but not excessive in relation to that purpose.

Data users are required to take all practicable steps to ensure that on or before the collection of the data subjects’ personal data (or on or before first use of the data in respect of item (d) below), the data subjects were informed of the following matters:

- the purpose of collection;
- the classes of transferees of the data;
whether it is obligatory to provide the data, and if so, the consequences of failing to supply the data; and

d the right to request access to and request the correction of the data, and the contact details of the individual who is to handle such requests.

Implications for organisations

A personal information collection statement (PICS) (or its equivalent) is a statement given by a data user for the purpose of complying with the above notification requirements. It is crucial that organisations provide a PICS to their customers before collecting their personal data. On 29 July 2013, the PCPD published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PICS. It is recommended that the statement in the PICS explaining what the purpose of the collection is should not be too vague and too wide in scope, and the language and presentation of the PICS should be user-friendly. Further, if there is more than one form for collection of personal data each serving a different purpose, the PICS used for each form should be tailored to the particular purpose.

DPP2 – accuracy and duration of retention

Principle

Under DPP2, data users must ensure that the personal data they hold are accurate and up to date, and are not kept longer than necessary for the fulfilment of the purpose.

After the Amendment Ordinance came into force, it is provided under DPP2 that if a data user engages a data processor, whether within 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 necessary for processing the data. ‘Data processor’ is defined to mean a person who processes personal data on behalf of a data user and does not process the data for its own purposes.

It should be noted that under Section 26 of the PDPO, a data user must take all practicable steps to erase personal data held when the data are no longer required for the purpose for which they were used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased. Contravention of this Section is an offence, and offenders are liable for a fine.

Implications for organisations

The PCPD published the Guidance on Personal Data Erasure and Anonymisation (revised in April 2014), which provides advice on when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and physical destruction. For example, it is recommended that dedicated software, such as that conforming to industry standards (e.g., US Department of Defense deletion standards), be used to permanently delete data on various types of storage devices. Organisations are also advised to adopt a top-down approach in respect of data destruction, and this requires the development of organisation-wide policies, guidelines and procedures. Apart from data destruction, the guidance note also provides that the data can be anonymised to the extent that it is no longer practicable to identify an individual directly or indirectly. In such cases, the data would no
longer be considered as ‘personal data’ under the PDPO. Nevertheless, it is recommended that data users must still conduct a regular review to confirm whether the anonymised data can be re-identified and to take appropriate action to protect the personal data.

**DPP3 – use of personal data**

*Principle*

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. ‘Prescribed consent’ means express consent given voluntarily and that has not been withdrawn by notice in writing.

*Implications for organisations*

Organisations should only use, process or transfer their customers’ personal data in accordance with the purpose and scope set out in their PICS. If the proposed use is likely to fall outside the customers’ reasonable expectation, organisations should obtain express consent from their customers before using their personal data for a new purpose.

**DPP4 – data security requirements**

*Principle*

DPP4 provides that data users must use all practicable steps to ensure that personal data held are protected against unauthorised or accidental processing, erasure, loss or use.

After the Amendment Ordinance came into force, it is provided under DPP4 that if a data user engages a data processor (such as a third-party IT provider to process personal data of employees or customers), whether within or outside Hong Kong, the data users must adopt contractual or other protections to ensure the security of the data. This is important, because under Section 65(2) of the PDPO, the data user is liable for any act done or practice engaged in by its data processor.

*Implications for organisations*

In view of the increased use of third-party data centres and the growth of IT outsourcing, the PCPD issued an information leaflet entitled ‘Outsourcing the Processing of Personal Data to Data Processors’, in September 2012. According to this leaflet, it is recommended that data users incorporate contractual clauses in their service contracts with data processors to impose obligations on them to protect the personal data transferred to them. Other protection measures include selecting reputable data processors, and conducting audits or inspections of the data processors.

The PCPD also issued the Guidance on the Use of Portable Storage Devices (revised in July 2014), which helps organisations to manage the security risks associated with the use of portable storage devices. Portable storage devices include USB flash cards, tablets or notebook computers, mobile phones, smartphones, portable hard drives and DVDs. Given that large amounts of personal data can be quickly and easily copied to such devices, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policies and practice. The guidance note recommended that a risk assessment be carried out to guide the development of an organisation-wide policy to manage the risk associated with the use of portable storage devices. Further, given the rapid development of technology, it is recommended that this policy be updated and audited regularly. Some
technical controls recommended by the guidance note include encryption of the personal
data stored on the personal storage devices, and adopting systems that detect and block the
saving of sensitive information to external storage devices.

**DPP5 – privacy policies**

**Principle**

DPP5 provides that data users must publicly disclose the kind of personal data held by them,
the main purposes for holding the data, and their policies and practices on how they handle
the data.

**Implications for organisations**

A privacy policy statement (PPS) (or its equivalent) is a general statement about a data user’s
privacy policies for the purpose of complying with DPP5. Although the PDPO is silent on the
format and presentation of a PPS, it is good practice for organisations to have a written policy
to effectively communicate their data management policy and practice. The PCPD published
a guidance note entitled Guidance on Preparing Personal Information Collection Statement
and Privacy Policy Statement, which serves as guidance for data users when preparing their
PPS. In particular, it is recommended that the PPS should be in a user-friendly language and
presentation. Further, if the PPS is complex and lengthy, the data user may consider using
proper headings and adopting a layered approach in presentation.

**DPP6 – data access and correction**

**Principle**

Under DPP6, a data subject is entitled to ascertain whether a data user holds any of his or her
personal data, and to request a copy of the personal data. The data subject is also entitled to
request the correction of his or her personal data if the data is inaccurate.

Data users are required to respond to a data access or correction request within
a statutory period of 40 days. If the data user does not hold the requested data, it must still
inform the requestor that it does not hold the data within 40 days.

**Implications for organisations**

Given that a substantial number of disputes under the PDPO relate to data access requests,
the PCPD published a guidance note entitled Proper Handling of Data Access Request and
Charging of Data Access Request Fee by Data Users, dated June 2012, to address the relevant
issues relating to requests for data access. For example, although a data user may impose a fee
for complying with a data access request, a data user is only allowed to charge the requestor
for the costs that are ‘directly related to and necessary for’ complying with a data access
request. It is recommended that a data user should provide a written explanation of the
calculation of the fee to the requestor if the fee is substantial. Further, a data user should not
charge a data subject for its costs in seeking legal advice in relation to the compliance with
the data access request.

**ii Direct marketing**

Hong Kong’s regulation of direct marketing deserves special attention from organisations
engaging in such activities. Unlike with violations of the DPPs, violations of the PDPO’s
direct marketing provisions are criminal offences, punishable by fines and by imprisonment. The PCPD has demonstrated a willingness to bring enforcement actions in this area and to refer particularly egregious violations for criminal prosecution.

**Revised direct marketing provisions under the PDPO**

The revised direct marketing provisions under the Amendment Ordinance entered into effect on 1 April 2013, and introduced a stricter regime that regulates the collection and use of personal data for sale and for direct marketing purposes.

Under the revised direct marketing provisions, data users must obtain the data subjects' express consent before they use or transfer the data subjects' personal data for direct marketing purposes. Organisations must provide a response channel (e.g., email, online facility or a specific address to collect written responses) to the data subject through which the data subjects may communicate their consent to the intended use. Transfer of personal data to another party (including the organisation's subsidiaries or affiliates) for direct marketing purposes, whether for gain or not, will require express written consent from the data subjects.

**Guidance on Direct Marketing**

The PCPD published the New Guidance on Direct Marketing in January 2013 to assist businesses to comply with the requirements of the revised direct marketing provisions of the PDPO.

**Direct marketing to corporations**

Under the New Guidance on Direct Marketing, the Privacy Commissioner stated that in clear-cut cases where the personal data are collected from individuals in their business or employee capacities, and the product or service is clearly meant for the exclusive use of the corporation, the Commissioner will take the view that it would not be appropriate to enforce the direct marketing provisions.

The Privacy Commissioner will consider the following factors in determining whether the direct marketing provisions will be enforced:

a. the circumstances under which the personal data are collected: for example, whether the personal data concerned are collected in the individual’s business or personal capacity;

b. the nature of the products or services: namely, whether they are for use of the corporation or for personal use; and

c. whether the marketing effort is targeted at the business or the individual.

**Amount of personal data collected**

While the Privacy Commissioner has expressed that the name and contact information of a customer should be sufficient for the purpose of direct marketing, it is provided in the New Guidance on Direct Marketing that additional personal data may be collected for direct marketing purposes (e.g., customer profiling and segmentation) if the customer elects to supply the data on a voluntary basis. Accordingly, if an organisation intends to collect additional personal data from its customers for direct marketing purposes, it must inform its customers that the supply of any other personal data to allow it to carry out specific purposes, such as customer profiling and segmentation, is entirely voluntary, and obtain written consent from its customers for such use.
Penalties for non-compliance
Non-compliance with the direct marketing provisions of the PDPO is an offence, and the highest penalties are a fine of HK$1 million and imprisonment for five years.

Spam messages
Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the Unsolicited Electronic Messages Ordinance (UEMO). Under the UEMO, businesses must not send commercial electronic messages to any telephone or fax number registered in the do-not-call registers. This includes text messages sent via SMS, pre-recorded phone messages, faxes and emails. Contravention of the UEMO may result in fines ranging from HK$100,000 to HK$1 million and up to five years' imprisonment.

In early 2014, the Office of the Communications Authority prosecuted a travel agency for sending commercial facsimile messages to telephone numbers registered in the do-not-call registers. This is the first prosecution since the UEMO came into force in 2007. The case was heard before a magistrate's court, but the defendant was not convicted because of a lack of evidence.

Person-to-person telemarketing calls
Although the Privacy Commissioner has previously proposed to set up a territory-wide do-not-call register on person-to-person telemarketing calls, this has not been pursued by the government in the recent amendment of the PDPO. Nevertheless, under the new direct marketing provisions of the PDPO, organisations must ensure that they do not use the personal data of customers or potential customers to make telemarketing calls without their consent. Organisations should also check that the names of the customers who have opted out from the telemarketing calls are not retained in their call lists.

On 5 August 2014, the Privacy Commissioner issued a media brief to urge the government administration to amend the UEMO to expand the do-not-call registers to include person-to-person calls. In support of the amendment, the Privacy Commissioner conducted a public opinion survey, which revealed that there had been a growing incidence of person-to-person calls, with more people responding negatively to the calls and fewer people reporting any gains from the calls. Although there had been long-standing discussions regarding the regulation of person-to-person calls in the past, it remains to be seen whether any changes will be made to the legislation.

Enforcement
Following prosecution referrals by the PCPD, Hong Kong courts handed down the first penalties in direct marketing violations in 2015. In September 2015, the Hong Kong Magistrates’ Court convicted the Hong Kong Broadband Network Limited (HKBN) for violating the PDPO’s requirement that a data user cease using an individual’s personal data in direct marketing upon request by that individual. The court imposed a fine of HK$30,000.

20 www.pcpd.org.hk/english/news_events/media_statements/press_20150909.html. HKBN appealed, and in 2017, the Hong Kong High Court dismissed the appeal, confirming that HKBN’s communication was for the purpose of direct marketing. See www.onc.hk/en_US/can-data-user-received-data-subjects-opt-request-
In a separate court action from September 2015, Links International Relocation Limited pleaded guilty to a PDPO direct marketing violation for not providing required information to a consumer before using his personal data in direct marketing.\(^{21}\) The court fined the company HK$10,000.

Additional convictions and fines followed in 2015 and 2016 for direct marketing violations. The most recent cases initiated by the PCPD resulting in fines and convictions were a January 2017 guilty plea by DBS Bank for failing to comply with a customer request to cease using personal data in direct marketing, resulting in a HK$10,000 fine,\(^{22}\) and a December 2016 guilty plea from a watch company that failed to obtain consent and to inform the consumer of his rights under the PDPO before engaging in direct marketing to the consumer, resulting in a HK$16,000 fine.\(^{23}\) Given the large number of criminal referrals by the PCPD with respect to direct marketing violations, we expect direct marketing prosecutions to continue to be an active enforcement area.

### iii  Technological innovation and privacy law

#### Cookies, online tracking and behavioural advertising

While there are no specific requirements in Hong Kong regarding the use of cookies, online tracking or behavioural advertising, organisations that deploy online tracking that involves the collection of personal data of website users must observe the requirements under the PDPO, including the six DPPs.

The PCPD published an information leaflet entitled ‘Online Behavioural Tracking’ (revised in April 2014), which provides the recommended practice for organisations that deploy online tracking on their websites. In particular, organisations are recommended to inform users what types of information are being tracked by them, whether any third party is tracking their behavioural information and to offer users a way to opt out of the tracking.

In cases where cookies are used to collect behavioural information, it is recommended that organisations preset a reasonable expiry date for the cookies, encrypt the contents of the cookies whenever appropriate, and do not deploy techniques that ignore browser settings on cookies unless they can offer an option to website users to disable or reject the cookies.

The PCPD also published the Guidance for Data Users on the Collection and Use of Personal Data through the Internet (revised in April 2014), which advises organisations on compliance with the PDPO while engaging in the collection, display or transmission of personal data through the internet.

#### Cloud computing

The PCPD published the information leaflet ‘Cloud Computing’ in November 2012, which provides advice to organisations on the factors they should consider before engaging in cloud computing. For example, organisations should consider whether the cloud provider has subcontracting arrangements with other contractors, and what measures are in place to ensure compliance with the PDPO by these subcontractors and their employees. In addition,
when dealing with cloud providers that offer only standard services and contracts, the data user must evaluate whether the services and contracts meet all security and personal data privacy protection standards they require.

On 30 July 2015, the PCPD published the revised information leaflet ‘Cloud Computing’ to advise cloud users on privacy, the importance of fully assessing the benefits and risks of cloud services and the implications for safeguarding personal data privacy. The new leaflet includes advice to organisations on what types of assurances or support they should obtain from cloud service providers to protect the personal data entrusted to them.

**Employee monitoring**

In April 2016, the PCPD published the revised Privacy Guidelines: Monitoring and Personal Data Privacy at Work, to aid employers in understanding steps they can take to assess the appropriateness of employee monitoring for their business, and how they can develop privacy-compliant practices in the management of personal data obtained from employee monitoring. The guidelines are applicable to employee monitoring activities whereby personal data of employees are collected in recorded form using the following means: telephone, email, internet and video.

Employers must ensure that they do not contravene the DPPs of the PDPO while monitoring employees’ activities. The PDPO has provided some additional guidelines on monitoring employees’ activities and has recommended employers to:

a. Evaluate the need for employee monitoring and its impact upon personal data privacy. Employers are recommended to undertake a systematic three-step assessment process:
   - ‘assessment’ of the risks that employee monitoring is intended to manage and weigh that against the benefits to be gained;
   - ‘alternatives’ to employee monitoring and other options available to the employer that may be equally cost-effective and practical but less intrusive on an employee’s privacy; and
   - ‘accountability’ of the employer who is monitoring employees, and whether the employer is accountable and liable for failure to be compliant with the PDPO in the monitoring and collection of personal data of employees.

b. Monitor personal data obtained from employee monitoring. In designing monitoring policies and data management procedures, employers are recommended to adopt a three-step systematic process:
   - ‘clarify’ in the development and implementation of employee monitoring policies the purposes of the employee monitoring; the circumstances in which the employee monitoring may take place; and the purpose for which the personal data obtained from monitoring records may be used;
   - ‘communication’ with employees to disclose to them the nature of, and reasons for, the employee monitoring prior to implementing the employee monitoring; and
   - ‘control’ over the retention, processing and the use of employee monitoring data to protect the employees’ personal data.

**IV PDPO AND INTERNATIONAL DATA TRANSFER**

Section 33 of the PDPO deals with the transfer of data outside Hong Kong, and it prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances,
such as where the data protection laws of the foreign country are similar to the PDPO or the data subject has consented to the transfer in writing. Section 33 of the PDPO has not been brought into force since its enactment in 1995, and although implementation has been consistently discussed in recent years, the government currently has no timetable for its implementation.

V PDPO COMPANY POLICIES AND PRACTICES

Organisations that handle personal data are required to provide their PPS to the public in an easily accessible manner. In addition, prior to collecting personal data from individuals, organisations must provide a PICS setting out, *inter alia*, the purpose of collecting the personal data and the classes of transferees of the data. As mentioned above, the PCPD has published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement (see Section III.i), which provides guidance for organisations when preparing their PPS and PICS.

The Privacy Management Programme: A Best Practice Guide (see Section II.i) also provides guidance for organisations to develop their own privacy policies and practices. In particular, it is recommended that organisations should appoint a data protection officer to oversee the organisation’s compliance with the PDPO. In terms of company policies, apart from the PPS and PICS, the Best Practice Guide recommends that organisations develop key policies on the following areas: accuracy and retention of personal data; security of personal data; and access to and correction of personal data.

The Best Practice Guide also emphasises the importance of ongoing oversight and review of the organisation’s privacy policies and practices to ensure they remain effective and up to date.

VI PDPO AND DISCOVERY AND DISCLOSURE

i Discovery

The use of personal data in connection with any legal proceedings in Hong Kong is exempted from the requirements of DPP3, which requires organisations to obtain prescribed consent from individuals before using their personal data for a new purpose (see Section III.i). Accordingly, the parties in legal proceedings are not required to obtain consent from the individuals concerned before disclosing documents containing their personal data for discovery purposes during legal proceedings.

ii Disclosure

Regulatory bodies in Hong Kong, such as the Hong Kong Police Force, the Independent Commission Against Corruption and the Securities and Futures Commission, are obliged to comply with the requirements of the PDPO during their investigations. For example, regulatory bodies in Hong Kong are required to provide a PICS to the individuals prior to collecting information or documents containing their personal data during investigations.

Nevertheless, in certain circumstances, organisations and regulatory bodies are not required to comply with DPP3 to obtain prescribed consent from the individuals concerned. This includes cases where the personal data are to be used for the prevention or detection of crime, and the apprehension, prosecution or detention of offenders, and where compliance with DPP3 would be likely to prejudice the aforesaid purposes.
Another exemption from DPP3 is where the personal data is required by or authorised under any enactment, rule of law or court order in Hong Kong. For example, the Securities and Futures Commission may issue a notice to an organisation under the Securities and Futures Ordinance requesting the organisation to produce certain documents that contain its customers’ personal data. In such a case, the disclosure of the personal data by the organisation would be exempted from DPP3 because it is authorised under the Securities and Futures Ordinance.

VII  PUBLIC AND PRIVATE ENFORCEMENT

i  Public enforcement

An individual may make a complaint to the PCPD about an act or practice of a data user relating to his or her personal data. If the PCPD has reasonable grounds to believe that a data user may have breached the PDPO, the PCPD must investigate the relevant data user. As mentioned above, although a contravention of the DPPs does not constitute an offence in itself, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

Prior to the amendment of the PDPO in 2012, the PCPD was only empowered to issue an enforcement notice where, following an investigation, it is of the opinion that a data user is contravening or is likely to continue contravening the PDPO. Accordingly, in previous cases where the contraventions had ceased and the data users had given the PCPD written undertakings to remedy the contravention and to ensure that the contravention would not continue or recur, the PCPD could not serve an enforcement notice on them as continued or repeated contraventions were unlikely.

Since the entry into force of the Amendment Ordinance, the PCPD has been empowered to issue an enforcement notice where a data user is contravening, or has contravened, the PDPO, regardless of whether the contravention has ceased or is likely to be repeated. The enforcement notice served by the PCPD may direct the data user to remedy and prevent any recurrence of the contraventions. A data user who contravenes an enforcement notice commits an offence and is liable on first conviction for a fine of up to HK$50,000 and two years’ imprisonment and, in the case of a continuing offence, a penalty of HK$1,000 for each day on which the offence continues. On second or subsequent conviction, the data user would be liable for a fine of up to HK$100,000 and imprisonment for two years, with a daily penalty of HK$2,000.

ii  Private enforcement

Section 66 of the PDPO provides for civil compensation. Individuals who suffer loss as a result of a data user’s use of their personal data in contravention of the PDPO are entitled to compensation by that data user. It is a defence for data users to show that they took reasonable steps to avoid such a breach.

After the Amendment Ordinance came into force, affected individuals seeking compensation under Section 66 of the PDPO may apply to the Privacy Commissioner for assistance and the Privacy Commissioner has discretion whether to approve it. Assistance by the Privacy Commissioner may include giving advice, arranging assistance by a qualified lawyer, arranging legal representation or other forms of assistance that the Privacy Commissioner may consider appropriate.
VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Although the PDPO does not confer extraterritorial application, it applies to foreign organisations to the extent that the foreign organisations have offices or operations in Hong Kong. For example, if a foreign company has a subsidiary in Hong Kong, the Hong Kong subsidiary will be responsible for the personal data that it controls, and it must ensure the personal data are handled in accordance with the PDPO no matter whether the data are transferred back to the foreign parent company for processing.

IX CYBERSECURITY AND DATA BREACHES

i Cybercrime and cybersecurity

As previously noted, Hong Kong does not have stand-alone cybercrime or cybersecurity legislation. The Computer Crimes Ordinance, which was enacted nearly 25 years ago in 1993, amended the Telecommunications Ordinance,24 the Crimes Ordinance25 and the Theft Ordinance,26 expanding the scope of existing criminal offences to include computer-related criminal offences. These include:

a unauthorised access to any computer; damage or misuse of property (computer program or data);

b making false entries in banks’ books of accounts by electronic means;

c obtaining access to a computer with the intent to commit an offence or with dishonest intent; and

d unlawfully altering, adding or erasing the function or records of a computer.

Although Hong Kong does not currently have cybersecurity legislation, the government does support a number of organisations dedicated to responding to cyber threats and incidents. These entities include the Hong Kong Emergency Response Team Coordination Centre (managed by the Hong Kong Productivity Council) for coordinating responses for local enterprises and internet users, and the Government Computer Emergency Response Team Hong Kong (a work unit established under the Office of the Government Chief Information Officer), which is a team charged with coordinating and handling incidents relating to both the private and public sectors. In addition, the Hong Kong Police Force has established the Cyber Security and Technology Crime Bureau, which is responsible for handling cybersecurity issues and combating computer crime.

ii Data breaches

There is currently no mandatory data breach notification requirement in Hong Kong. In October 2015 and then again in December 2016, the PCPD revised its Guidance on Data Breach Handling and the Giving of Breach Notifications, which provides data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the individuals involved. Although the PCPD noted in the Guidance that there are no statutory notification requirements, the PCPD recommended that data users strongly consider

24 Sections 24 and 27 of the Telecommunications Ordinance.
25 Sections 59, 60, 85 and 161 of the Crimes Ordinance.
26 Sections 11 and 19 of the Theft Ordinance.
notifying affected persons and relevant authorities, such as the PCPD. In particular, after assessing the situation and the impact of the data breach, the data users should consider whether the following persons should be notified as soon as practicable:

- the affected data subjects;
- the law enforcement agencies;
- the Privacy Commissioner (a data breach notification form is available on the PCPD’s website);
- any relevant regulators; or
- other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the data subjects affected (e.g., internet companies such as Google and Yahoo! may assist in removing the relevant cached link from their search engines).

X OUTLOOK

Hong Kong’s data privacy and protection framework is long-standing and relatively mature. We expect that the PCPD will continue enforcement at generally the same levels, with continued emphasis on direct marketing violations and prosecution referrals for such violations.

In recent public statements, the PCPD has noted the passage of China’s cybersecurity legislation and the impending implementation of the EU’s General Data Protection Regulation, and underscored the importance of Hong Kong as a cross-border data transfer bridge between China and the EU. We expect that the PCPD and the Hong Kong government will continue to emphasise the development of Hong Kong as Asia’s premier data hub and to provide additional policy, promotional and incentive support to facilitate growth in the region.

With respect to cybercrime and cybersecurity, we do not anticipate major legislation in the near term and expect that sectoral regulators will continue to take the lead in these areas.
Chapter 13

HUNGARY

Tamás Gödölle

I OVERVIEW

The new constitution of Hungary (the Fundamental Law) was adopted in 2011 and entered into force on 1 January 2012. The Fundamental Law contains a section on ‘Freedom and Responsibility’, which describes the fundamental rights of individuals. Article VI(1) of the Fundamental Law generally provides that everyone is entitled to respect for his or her private and family life, home, communications and good reputation, whereas Article VI(2) provides for the right to the protection of personal data as well as for the right to access and disseminate information of public interest. In addition, Article VI(3) states that an independent authority shall be responsible for the enforcement of the protection of personal data and freedom of access to data of public interest.

The Hungarian Civil Code, which was adopted in 2013 and entered into force on 15 March 2014, also contains provisions concerning privacy rights. The general rules on the protection of personality rights (including the right for the protection of personal data) are set out in the Civil Code, which provides the basic rules for civil law relationships. Accordingly, personality rights can be exercised freely within the framework of the law and within the rights of others. The exercise of such rights shall not be impeded by any other person. However, personality rights shall not be considered as having been violated if the person has given prior consent.

Although the above legislation contains most general principles and clauses, Hungary has a single legislative privacy regime. The general rules of the protection of personal data and freedom of information are governed by Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the Privacy Act). The Privacy Act implemented the European Data Protection Directive 95/46 Directive and lays down the general rules for the protection of personal data of individuals in Hungary.

The entity responsible for enforcing the data protection law is the Data Protection and Freedom of Information Authority (DPA). The DPA aims to guarantee the rights of individuals to exercise control over their privacy and to have access to data of public interest and public data on the grounds of public interest. The Privacy Act is regarded as background legislation for specific statutes regulating the collection and processing of personal data.

The Privacy Act should be considered as the general Act providing rules regarding the protection of personal data and the disclosure of public data. Beyond the scope of the Privacy

---

1 Tamás Gödölle is a partner at Bogsch & Partners Law Firm.
2 The translation of the consolidated version of the Fundamental Law of Hungary is available at www.kormany.hu/download/e/02/00000/The%20New%20Fundamental%20Law%20of%20Hungary.pdf.
Act, there are other sectoral acts (e.g., the Labour Code, Electronic Communications Act, etc.) that provide additional data protection-related provisions. The processing of medical, criminal, electoral and citizenship data is regulated by other acts.

In Hungarian data privacy regulation, the role of NGOs and self-regulatory industry groups, as well as society or advocacy groups, is marginal, and there are no specific Hungarian laws providing for government surveillance powers.

The government approved the National Cybersecurity Strategy, which determines the national objectives and strategic directions, tasks and comprehensive government tools to enable Hungary to enforce its national interests in Hungarian cyberspace, within the context of the global cyberspace. The strategy aims at developing a free and secure cyberspace and at protecting national sovereignty.

II THE YEAR IN REVIEW

The year 2017 has been approached in the spirit of preparing for the new regime that the General Data Protection Regulation (GDPR) will bring as of May 2018, and has seen many related publications and opinions issued by private sector market participants; however, there have been no truly significant materials made public by the DPA as of the end of August 2017.

As a first-wave preparation aid, the DPA published a localised version\(^3\) of the UK Information Commissioner’s Office’s 12-point list on how to get ready for the GDPR. Subsequently, in its annual report,\(^4\) the DPA dedicated a whole chapter to analysing and describing the most important developments of the GDPR, and even provided comparisons with the local Privacy Act to explain the key changes that the GDPR will introduce when it enters into force.

Slightly late but still in due time at the end of August 2017, a bill of law has been submitted to parliament with the aim of harmonising the Privacy Act with the new – directly applicable – GDPR. The general and detailed debate on the bill, and hopefully its adoption, will take place during the autumn parliamentary session.

In early 2017, the DPA reassigned a number of its personnel to start preparations for the GDPR. Unfortunately, as a result, the other DPA departments dealing with actual pending cases suffered a drastic manpower shortage and a significant backlog of cases piled up. By late spring the shortage of labour had resulted in serious delays (measurable in months) in the DPA’s decision-making and issuing processes. Moreover, the prompt management of cases and processing of submissions were further hindered by the fact that the DPA started monitoring the submissions (e.g., data protection notifications) more thoroughly.

Fortunately, the DPA managed to overcome the aforesaid difficulties by late summer.

---

The Privacy Act regulates the protection of personal data in Hungary. The Act, which was enacted in 2011 and entered into force on 1 January 2012,\(^5\) purports to guarantee the right of everyone to exercise control over his or her personal data and to have access to data of public interest.

The Privacy Act distinguishes two categories of protected information: ‘personal data’ and ‘sensitive data’. There is also a third category of personal data named ‘data of public interest’.

**Personal data**

The Privacy Act applies to all data processing and technical data processing that is carried out in Hungary, and that pertains to the data of natural persons or that contains data of public interest or ‘data public on grounds of public interest’.\(^6\) The Privacy Act regulates the processing of data carried out wholly or partially by automatic means, and the manual processing of data.

Personal data are defined in Article 3.2 of the Act as any data relating to the data subject – a specific (directly or indirectly identified or identifiable) natural person – and any conclusion with respect to the data subject that can be inferred from that data, in particular by reference to his or her name, identification code or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

**Sensitive data**

The term ‘special data’ (sensitive data) is defined as information on a data subject’s racial and national origin, political opinion or party affiliation, religious or ideological beliefs, or membership of any special interest organisations, as well as his or her state of health, pathological addictions, sex life or criminal personal data.\(^7\)

The Privacy Act also protects data of public interest and data that are public on grounds of public interest. The term ‘data of public interest’ is defined to include any information or knowledge, not falling under the definition of personal data, processed by an organ or person performing a state or local government function or other public function determined by a rule of law.\(^8\)

**Data controller**

A data controller has been defined by the Privacy Act as any natural or legal person, or any organisation without legal personality, who or which, alone or jointly with others, determines the purpose of the processing of personal data, makes decisions on data processing (including those as to the means of the processing), and implements these decisions or has them implemented by the technical data processor he or she has assigned.

---


\(^6\) Data Protection Law, Article 1.

\(^7\) Ibid., Article 3(3).

\(^8\) Ibid., Article 3(5).
The Act identifies a ‘technical data processor’ as any natural or legal person or organisation without legal personality that carries out the technical processing of personal data based on a contract with the data controller – including the conclusion of a contract pursuant to a rule of law.

**Data processor**

The Act applies to both types of data processing entities, namely data controllers and technical data processors, with some different provisions applying to technical data processing.

The data controller is always responsible for the lawfulness of the instructions given for the data processing operations of its outsourced (technical) data processor.

The technical data processor shall process personal data in compliance with the special instructions of the data controller; consequently, he or she cannot make any decisions concerning data processing.

It has been noted that, as of 1 July 2013, a data processor may contract out processing operations to another processor in line with the instructions of the data controller.

**Data protection audits**

With effect from 1 January 2013, the DPA provides data protection audits as a service to data controllers who request it. The DPA may charge an administrative fee for the audit that cannot exceed 5 million forints. The relevant aspects of DPA audits have been published on the DPA’s website.

**Protection of consumers**

The Direct Marketing Act identifies numerous obligations for marketing organisations to ensure the protection of consumers, and particularly restricts the use of the name and home address of natural persons for marketing purposes. Notably, the provisions of the Direct Marketing Act are only applicable where the marketing materials are sent by post. Marketing materials sent by electronic means are regulated by the Advertising Act and the e-Commerce Act.

**General obligations for data handlers**

According to the Privacy Act, personal data may not be processed unless the data subject has given his or her prior consent, or if an exception applies or the provision and processing of personal information is ordered by a law or – based on the parliamentary Act – by a local government decree.

Before collecting information from an individual, an organisation must indicate to the data subject whether data processing is based on consent or is compulsory. In addition, the data controller must provide the data subject with unambiguous and detailed information on all the facts relating to the processing of his or her data.

Regarding online data, Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services provides, *inter alia*, that information means any data, signal or image that can be processed, stored and transmitted by electronic means.
irrespective of whether its content is protected by law; and information society service means remote services provided by electronic means, generally for payment, and accessed by the recipient of the service individually.

According to this Act, the service provider may process personal data that is suitable and sufficient for the identification of the recipient of the service for the purposes of:

- drawing up a contract for the service in question;
- determining and modifying the contents and monitoring the performance of the service;
- charging for the service; and
- enforcing claims relating to the service.

The recipient of the service shall be allowed – at all times before and during the course of using the information society service – to prohibit the data processing.

Requirements of preliminary notices

As mentioned above, data controllers must provide data subjects with unambiguous and adequately detailed information on the circumstances of the processing of his or her personal data. Although the Privacy Act does contain provisions to this respect, on 9 October 2015, the DPA issued an official recommendation regarding the minimum requirements for preliminary notices provided to data subjects prior to the commencement of the processing of their personal data. While these recommendations are generally considered as soft law, in the event of an investigation, the DPA will check whether the data controller meets these requirements.

The recommendation sets out general principles regarding the quality and accessibility of notices, and also contains explanations pertaining to the applicable provisions of the Privacy Act. According to the recommendation, preliminary notices shall:

- be clear: repeating the words of the Privacy Act is not adequate, and the use of everyday wording is suggested;
- be readable and comprehensible: the text of the notice shall be structured and easy to understand;
- align with the set of concerned data subjects: if during the course of the data processing the set of data subjects can be easily determined, then the notice shall align with the specific requirements of the data subjects;
- not be considered a legal statement: the notice itself is not a legal statement. However, the information therein may have a greater impact on the data subjects’ consent (which is a legal statement). Should the notice be considered a legal statement, its clarity and transparency would be weakened by the details required by law;
- describe unique data processing: the document fulfils its role as a notice if it contains the unique data processing regulations concerning the specific data controller; and
- be available and accessible: the notice shall always be accessible for the data subject at the time when his or her personal data are being collected.

Data security incident register

According to Article 15(1a) of the Privacy Act, for subsequent countermeasure examinations by the DPA and for data subject notification purposes, the data controller shall keep a record of all data regarding data security incidents. The register shall contain:

- the personal data concerned;
- the scope and number of subjects affected by the data security incident;
- the date, time, circumstances and effects of the incident; and
- countermeasures carried out.

Database registration requirements

Article 65 of the Privacy Act requires data controllers to notify the DPA of their activities before they process personal data. Hungarian law requires the disclosure of a wide range of information.

The DPA maintains a register of data processing activities (the Registry). If notification of data processing is required to be given to the Registry, data processing may be commenced only after the registration has taken place. As a rule, no authorisation from the DPA is necessary (with the exception of client-related data processing activities of financial service providers and public utility and telecommunications companies), and processing may commence upon confirmation from the DPA or, as a rule, in the absence of confirmation, on the ninth day following submission of the notification to the Registry.

When registering for the first time, each data controller receives a registration number, which must be used whenever data is transferred, made public or supplied to the data subject.

There are numerous exceptions to the obligation to notify the DPA. These include, for example, where data processing operations involve the data of persons having an employment, membership, student or customer relationship with the data controller, or data collected for granting financial or social assistance to the data subject, or data registering such assistance.

Rights of data subjects

Under Article 15 of the Privacy Act, data subjects may request information on the processing of their personal data, such as which data are processed by the data controller or its data processors; about the purpose of the processing, its legal basis, its duration and the name, address and activity of the data processor; and, should there be one, on the circumstances of any data protection incident. They also have the right to know who has received or will receive their data, and for what purpose. Except for compulsory data processing, data subjects also have the right to have their data rectified or deleted (unless the data was collected pursuant to a law). The data controller must give this information within 25 days and in an easily understandable manner. Data controllers must provide this information in written form if this is requested by the data subject.

The Privacy Act requires data controllers to rectify any inaccurate personal data. In addition, it provides for the deletion of personal data if the processing is unlawful, if this has been requested by the data subject, or if this has been ordered by a court or the DPA.
A data controller must delete data that is incomplete or inaccurate and cannot be corrected in a lawful way, unless the deletion is prohibited by another law. It must also destroy data when the purpose of processing has ceased to exist, or when the time limit for the storage of the data has expired.

**Right to objection**

Article 21 of the Privacy Act grants data subjects the right to object to the processing of their data in numerous circumstances. These include, for example, when the processing is necessary only for enforcing a right or legitimate interest of the data controller or third party, unless the data processing has been ordered by law.

When an objection has been filed, the data controller must suspend the use of the data while investigating the complaint. It must respond to the request promptly, within 15 days.

**Redress and enforcement rights**

Any individual may file a complaint with the DPA if he or she thinks that his or her rights have been violated, or that there is an imminent danger of such a violation, except when judicial proceedings are already pending concerning the case in question. Article 52 of the Privacy Act protects the persons who made the complaint or reported to the DPA, and provides that they shall not suffer any prejudice because of their reporting to the DPA, and that they shall enjoy the same protection as persons making reports of public interest.

From 1 October 2015, the maximum sum of a data protection fine that can be imposed upon a person or entity responsible for a data security incident increased to 20 million forints. Data controllers are held liable under the Privacy Act for any damage suffered by data subjects as a result of the unlawful processing of their data or the infringement of the data protection requirements in the Privacy Act. As of 15 March 2014, the data subject may also claim exemplary damages – namely, lump sum damages that can be awarded by the court as compensation for harm sustained from the infringement of privacy rights by the data controller as a result of unlawful data processing or a breach of data security requirements.

iii **Technological innovation and privacy law**

More detailed regulatory frameworks apply to several data privacy issues.

**Employee monitoring**

The Labour Code generally authorises employers to introduce monitoring measures.\(^{17}\) It allows employers to monitor the conduct of employees; however, such measures may be taken only in the context of employment. Further, the means used for monitoring may not violate the human dignity of the worker. To exclude all possibility of doubt, the Labour Code also states that the private life of the employee cannot be monitored, which is in conformity with the practice of the European Court of Human Rights. In addition, the employer must give notice to employees, in advance, of the use of technical means serving to control or monitor employees’ conduct.

---

\(^{17}\) Labour Code, Article 11.
On 30 January 2013, the DPA issued a recommendation on video surveillance in the workplace, which addresses the issues of legal basis, guarantees, data retention, notice and registration requirements relating to the operation of surveillance systems.18

Based upon the DPA’s recommendation, if video surveillance involves or affects third parties (such as visitors), the DPA must be notified of the data processing relating to the surveillance system. Notification and registration are also required if the surveillance system is not operated by the employer directly, but by a service provider (security service) that is considered the sole controller of the system.

On 28 October 2016, the DPA issued a guideline concerning the basic requirements for workplace data processing operations.19 The guideline consists of two major parts, the general principles and the special rules for specific data processing operations.

In the first chapter, the guideline compares the principles (purpose, limitation, necessity and proportionality) of the Privacy Act and the Labour Code, and concludes with a joint interpretation of them with respect to workplace data processing activities. Certain privacy-related legal constructs are also explained from a labour law point of view, such as the legal basis of the data processing (consent, mandatory processing, and legitimate interest), the requirement to provide privacy notices to the data subjects prior to the commencement of processing, and cross-border transmission of employee personal data.

The second chapter of the guideline contains basic requirements concerning data processing operations for the following purposes:

\[ a \] job applications (including anonymous job applications);
\[ b \] monitoring applicants’ social media history;
\[ c \] retention of applications and CVs;
\[ d \] data processing by private employment agencies;
\[ e \] aptitude tests;
\[ f \] ability to require a clean criminal record from employees;
\[ g \] workplace CCTV surveillance;
\[ h \] monitoring the use of corporate email accounts;
\[ i \] monitoring the use of corporate portable devices (laptops and notebooks);
\[ j \] monitoring internet usage on corporate devices;
\[ k \] monitoring the use of corporate mobile phones;
\[ l \] applicability of use and implementation of GPS navigation systems;
\[ m \] applicability of use and implementation of biometric systems; and
\[ n \] requirements for the operation and maintenance of whistle-blowing systems.

**Restriction on cookies**

In November 2009, the European Commission adopted Directive 2009/136/EC (2009 Directive), and this amendment was to be implemented in the laws of each of the European Union Member States by 25 May 2011.

Article 3(5) of the 2009 Directive was implemented in Hungary by Section 155(4) of the Hungarian Act on Electronic Communications, which generally provides that data may

18 The guidance is available in Hungarian at http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelésr-l.pdf.
be stored or accessed on the terminal equipment of the subject end-user or subscriber after
the provision of clear and comprehensive information, including the purpose of the data
processing, if the corresponding consent of the end-user or subscriber has been granted.

**Cloud Computing Circular released by the HFSA**

The Hungarian Financial Supervisory Authority (HFSA) – which merged with the Central
Bank of Hungary on 1 October 2013 – released an executive circular (4/2012)\(^{20}\) on the
risks of public and community cloud services used by financial institutions, namely banks,
insurance companies and financial service providers in Hungary. The executive circular
qualifies the use of cloud services by financial institutions as ‘outsourcing’, and notes that
sectoral legislative rules shall be considered. Accordingly, the cloud service provider shall
comply with the same requirements applicable to financial institutions in terms of personnel,
material and security conditions.

The HFSA advises financial institutions to take into account, in a proportionate
manner, the risks of outsourcing, and to choose a provider and the technical means of
outsourcing accordingly. The HFSA announced that it would examine the legal compliance
of the technical and contractual implementation of the use of cloud services in on-site audits.

**Location tracking in relation to employment**

According to the most recent information from the DPA, data collected through GPS or
GSM base stations is only lawful if any device used to collect location data has a function
allowing the employee to turn the device off outside business hours. Employers may then
be able to justify their collection of the location data during business hours as continuous
monitoring is considered to be unlawful.

**Automated profiling, facial recognition technology and big data**

Although the EU Article 29 Working Party has published opinions on automated profiling,
facial recognition technology and big data, the DPA has not yet published any guidelines on
these matters.

**iv Specific regulatory areas**

**The protection of children**

The Privacy Act provides that children over 16 are able to give consent without additional
parental approval. Obviously, this facilitates the processing of data relating to younger people.
It is important to note that, according to the new EU Data Protection Regulation, in future,
children under 18 will not be competent to give consent without parental approval.

**Health**

The processing of health data is governed by the provisions of the Act on Medical Care
(Act CLIV of 1997) as well as by the Act on Handling and Protecting Medical Data
(Act XLVII of 1997). The processing of human genetic data (and research) is governed by
the Act on the Protection of Human Genetic Data and the Regulation of Human Genetic
Studies, Research and Biobanks.

The Act on Handling and Protecting Medical Data uses a very broad definition of ‘health data’. In the Act, health data are defined as:

a any data relating to the data subject’s physical, emotional or mental status, pathological addiction, as well as the circumstances associated with disease, death or cause of death that is communicated by the data subject or by any third person in relation to the data subject, or experienced, examined, measured, extracted by or relating to the medical health service; and

b any data in connection with or affecting the health service (including, for instance, any conduct, environment or profession). Since health data are covered by the definition of ‘special data’ under the Privacy Act, the processing of such personal information is only permitted with the written informed consent of the data subject or if explicitly ordered by the act of legislation.

The Act on Handling and Protecting Medical Data identifies the legal purposes for which health data may be processed.

For any other purposes not covered explicitly by the provisions of the Act, health data and the related personal identification data may only be processed if the patient, or his or her legal or duly authorised representative, granted his or her informed, written consent to the processing.

The Act determines the scope of persons who may lawfully process health data. The Act also regulates the strict secrecy obligations of medical personnel providing medical treatment. Medical institutions must store health records for 30 years and must store final reports for 50 years, after which time the documentation must be destroyed.

Patients have the right to be informed about the handling of their health data. They also have the right to access their health data.

Electronic communications

Under the provisions of the Electronic Communications Act of 2003, service providers are generally authorised to process the personal data of end-users and subscribers, always to the extent required and necessary:

a for their identification for the purpose of drawing up contracts for electronic communication services (including amendments to such contracts);

b to monitor performance;

c for billing charges and fees; and

d for enforcing any related claims.

Further, the Act provides that the provision of electronic communications services may not be made dependent upon the user’s consent for processing his or her personal data; the Act on Electronic Communications defines other purposes for processing personal data.21

Commercial communications

Several laws address the protection of personal data in the context of commercial communications. These laws include Act CVIII of 2001 on Electronic Commerce and on

21 Act on Electronic Communications, Article 154(6).
Information Society Services (the e-Commerce Act),22 the 1995 Law on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (the Direct Marketing Act), as well as the 2008 Act on the Basic Requirements and Certain Restrictions of Commercial Advertising Activity (the Advertising Act).

In 2001, Hungary enacted the e-Commerce Act, which requires that each commercial email clearly and unambiguously indicates that a commercial message is an electronic advertisement, and that it provides the identity of the electronic advertiser or that of the actual sender.23

The Advertising Act provides that unsolicited marketing material may not be sent to an individual without having obtained the prior, express, specific, voluntary and informed consent of the individual in compliance with the applicable provisions of the Privacy Act.24 The message must contain the email address and other contact details where the individual may request the prohibition of the transmission of electronic advertisements.25

The advertiser, advertisement service provider and publisher of electronic advertisements are required to keep a register of persons who have given their consent to receiving advertisements.26 The information about these individuals may be disclosed to any third party solely upon the prior consent of the individual. Advertisers may send advertisements through email or equivalent means (e.g., text messages) to those who are listed in the register.

The Direct Marketing Act significantly restricts the use of the name and home address of natural persons for marketing purposes.27 Only a limited number of means may be used to obtain the contact details of natural persons for establishing contact (permission email). These sources include business contacts as well as phone books or statistical name listings, provided that the data subjects were informed at the time of the data gathering, and advised regarding the possibility that the data might be used for purposes other than originally intended, and of their right to prohibit such use.28

IV INTERNATIONAL DATA TRANSFER

The Privacy Act defines the term ‘transfer’ as making data accessible to a specific third party, namely, where data are passed on. The Privacy Act defines a ‘third party’ as any natural or legal person or organisation without legal personality, other than the data subject, the data controller or the technical data processor. It follows therefore that the transfer does not include data transfers between the data subject, the data controller or the technical data processor.

Data transfers within the Member States of the EEA are treated as a domestic data transfer.

The Privacy Act permits the transfer of personal data to a data controller or to a data processor processing personal data in a third country:

a if the data subject explicitly consents to such a transfer;

22 The e-Commerce Act is available in Hungarian at http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv.
23 e-Commerce Act, Article 14/A.
24 Ibid., Article 14(2).
25 Ibid., Article 14(3).
26 Ibid., Article 14(5).
27 Direct Marketing Act, Section 5.
28 Ibid., Section 3(1)(b).
in the event of emergency situations or in the vital interest of the data subject or a third person; or

for the execution of an international agreement on mutual legal assistance if an adequate level of protection of personal data is ensured.

The adequate level of protection can be ensured:

a by a binding legal act of the European Union;

b by an international agreement between the third country and Hungary containing guarantees for the rights of data subjects and for the independent supervision of data control and data processing operations; and

c if the data controlling and data processing procedures comply with binding corporate rules.29

V COMPANY POLICIES AND PRACTICES

There are no official codes of practice regarding company policies and practices. However, preparing internal privacy policies under Hungarian law is mandatory in some cases, such as for financial institutions, public utility companies or electronic communications service providers, which are all required to introduce internal data protection guidelines, setting out the relevant company’s compliance programme in accordance with the provisions of the Act. Nevertheless, it is also common that companies that do not fall under such an obligation – especially multinational companies who process cross-border data flows both within and outside their company group – still introduce internal privacy policies and publish privacy notices. In any case, policies containing information relating to the processing of personal data shall comply – beyond the applicable regulations of the Privacy Act – with the requirements determined by the DPA in its official recommendation of 6 October 2015 regarding privacy notices.


Under the section ‘Protection of Personal Rights’, Article 9 of the Labour Code generally articulates that everyone shall respect the personal rights of persons covered by the Act. Employers must provide notice to their employees on the processing of their personal data. Employers may only disclose facts, data and opinions concerning an employee to third persons in those cases specified by law or with the employee’s consent.

The Labour Code generally authorises employers to introduce monitoring measures. The Code provides that an employer may monitor the conduct of employees; however, such measures may be taken only in the context of employment, and the means used for monitoring may not violate the human dignity of the worker. In addition, the employer must give notice to the employee in advance of the use of technical means to control or monitor the employee’s conduct. As regards a worker’s consultation and information, the Labour Code provides that employers must consult with works councils before implementing measures and internal regulations affecting large numbers of employees. That information obligation covers, inter alia, the processing and protection of personal data of employees as well as the use of technical measures used for employee monitoring.

29 Implemented in 2015. Applicable from 1 October 2015.
Restricting employee personal rights, however, is legitimate only if it matches the requirements of necessity and proportionality, namely if the restriction is definitely necessary because of a reason arising from the employment relationship and if the restriction is also proportionate for achieving its objective.

i Whistle-blowing system

Regarding the processing of employee data in whistle-blowing systems, Act CLXV of 2013 on Complaints and Public Interest Disclosure lays down the relevant rules.

The Act authorises employers to establish a system to investigate whistle-blowing reports. Conduct that may be reported includes the violation of laws as well as codes of conduct issued by the employer, provided that these rules protect the public interest or significant private interests.

The employer must publicly disclose on its corporate website the rules of conduct the violation of which may be subject to reporting, and a detailed description of the reporting procedure in Hungarian.

The investigation of a report is mandatory for employers, and the reporting person must be informed of the outcome of the investigation and of the measures taken. The identity of the reporting person may not be disclosed without his or her consent. The Act permits the receipt and investigation of anonymous reports; however, the deadline for the investigation of such reports cannot be extended.

According to the Labour Code, employers must consult with works councils before implementing measures and internal regulations affecting large numbers of employees. This would include the implementation of a modified or new whistle-blowing system.

ii Specific provisions relating to credit data

The processing of personal data, business secrets and bank secrets by financial institutions (namely, by credit institutions and financial undertakings), data security requirements as well as data processing within the framework of the Central Credit Information System are regulated by Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings (the Banking Act).

Under the provisions of the Banking Act, credit institutions are authorised to outsource the activities connected to financial services and activities auxiliary to financial services, as well as those statutory activities prescribed by law that involve the processing of data, provided that outsourcing complies with data protection provisions. Accordingly, the outsourcing service provider must satisfy – to a degree corresponding to the risk – the personnel, infrastructure and security requirements concerning the outsourced activities that are prescribed by law for credit institutions. The Banking Act also lays down mandatory provisions for the outsourcing contract.

iii Genetic data

The processing of human genetic data is governed by Act XXI of 2008 on the Protection of Human Genetic Data and the Regulation of Human Genetic Studies, Research and Biobanks, which entered into effect on 1 July 2008. The general rules of the Act lay down that human genetic data may only be used either for the purpose of human genetic research or for medical examination. The Act guarantees the data subject’s right of information self-determination in connection with human genetic data, as it requires the written informed consent of the data subject for such data processing.
iv Internal data protection officer

The Privacy Act provides that selected data controllers, such as public administrative bodies, financial organisations, public utilities companies and communications companies, that customarily process huge amounts of personal data are obliged to appoint an internal data protection officer, working under the direct control and supervision of the respective data controllers’ general manager. Among the data protection officer’s various tasks, he or she is specifically responsible for:

- contributing to or assisting in decision-making related to data processing and to the enforcement of the rights of data subjects;
- monitoring compliance with the Privacy Act and other rules of law on data processing, as well as with the provisions of internal data protection and data security rules and requirements;
- investigating reports submitted to him or her; and
- providing the data controller or technical data processor with information relating to the detection of any unlawful data processing activities.

Pursuant to the implementation of data security incidents in the Privacy Act, the internal data protection officer shall manage the data security incident register, which contains records of incidents.

VI DISCOVERY AND DISCLOSE

The Hungarian Governmental Control Office, which is responsible for the control of the state budget, launched a widespread investigation into the use of the money originating from the state of Norway that is handled by the Norwegian Fund in Hungary. Through the Fund, Norway pays a certain sum (amounting to billions of forints) to Hungarian NGOs and civil organisations in line with Norway’s agreement with the EU in exchange for its customs-free access to the European market. It is debatable whether these funds are to be considered as part of the Hungarian or Norwegian budget, and therefore it is also debatable whether the Hungarian Governmental Control Office has jurisdiction over this. The Control Office requested certain data from the relevant NGOs, which were cooperative despite the unclear legal background. Although Norway had objected to the audit, the audit continued, and further documents and data were requested by the Control Office.

Finally, Hungarian and Norwegian officials agreed to undertake certain financial controlling measures. Thus, on 9 December 2015, Norway lifted the suspension of payments to Hungary (which had been ordered on 7 May 2014). Accordingly, Hungarian NGOs may again access the subsidies of the Norwegian Fund.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA plays a key role in the enforcement of the protections of the Privacy Act. The DPA is responsible both for the supervision and enforcement of compliance with the Privacy Act and other data protection and data processing laws as well as freedom of information laws in Hungary. Hungarian data protection and privacy laws are enforced by the DPA and the Hungarian courts. No other organisations have an official role in data protection regulation.
The DPA monitors the conditions of the protection of personal data and investigates complaints. Representatives of the DPA may enter any premises where data are processed. If they observe any unlawful data processing, they have the authority to make the data controller discontinue the processing. The administrative procedure of the DPA is governed by the General Provisions of the Act on Administrative Procedure and, in the event of breach of the material provisions of the Act, the DPA is empowered to:

a. request that an entity cease and desist from infringing the law;

b. order the blocking, deletion or destruction of unlawfully processed data;

c. prohibit the unlawful processing;

d. suspend the transfer of data to foreign countries; and

e. impose a fine of up to 20 million forints.

Under the Act, the data controller, data processor and data subject are all entitled to appeal to the court to contest an order of the DPA. Pending a final and binding decision of the court, the data concerned must not be erased or destroyed, but processing of the data must be suspended and the data blocked. Moreover, the general rights of appeal under the Civil Procedure Act will still apply.

The DPA may initiate criminal proceedings with the body authorised to launch such proceedings if it suspects that an offence has been committed during the course of the procedure. The DPA shall initiate infringement or disciplinary proceedings with the body authorised to launch such proceedings if it suspects that an infringement or disciplinary violation has been committed during the course of the procedure.

The Privacy Act has established the Conference of Internal Data Protection Officers, which is headed by the president of the DPA and secures the information exchange between data protection officers.

ii Recent enforcement cases

The DPA did not publish any action plans for 2017 to indicate what topics it considered important. However, the investigational pattern of the DPA shows that in the current year the monitoring of international data transfers and data processing operations for credit management and financial purposes have been priorities.

In one case, the DPA investigated the legitimacy of the cross-border data transfer practices of a company established in France. The company had implemented binding corporate rules (BCRs) to legitimise data transfers within the company group across the globe and subsequently filed these BCRs with the French Data Protection Authority (CNIL) for validation. Upon receiving CNIL approval, the company was listed on the relevant European Commission website as an entity using BCRs. The Hungarian DPA, however, detected ex officio that although the company had also requested approval for Hungary, it had failed to submit its BCRs to the local DPA for approval. Under the Privacy Act, BCRs may only be used as an adequate safeguard for international data transfers upon approval by the local DPA. The DPA established that, in the absence of local approval for the BCRs, the data transfers of the company had been unlawful and – without imposing any penalties – ordered the company to submit its BCRs to the Hungarian DPA without further delay.

30 NAIH/2016/5859/H.
In another case, the DPA investigated the data processing activities of a medium-sized company active in the consumer credit business. The DPA established that the company’s data processing practices had been unlawful as the company had violated the principles of data minimisation and purpose limitation (by collecting and retaining copies of customer identification documents), had violated its obligations concerning preliminary notification of customers (by not informing customers on all aspects of the data processing) and had also processed customer personal data without a proper legal basis. Consequently, the DPA imposed a data protection fine amounting to 1 million forints.

There have also been some developments in an enforcement case mentioned last year. In this case, the DPA had established that Budapest City Archives violated the right to the protection of the criminal personal data of a formerly popular sports trainer by releasing information on a criminal judgment relating to him; the DPA imposed a data protection fine on the City Archives amounting to 3 million forints.

In the course of an appeal procedure, the case was brought before the Administrative and Labour Court of the Budapest-Capital Regional Court. In its final judgment, the Court established that the City Archives had acted legally in allowing access to anonymised documents and giving out the criminal judgment in question. Strangely, the Court did not order the DPA to recommence its procedure, and instead repealed fully the DPA’s decision.

iii  Private litigation

In the event of infringement of his or her rights, a data subject may file a court action against a data controller. In the court proceeding, the data controller bears the burden of proving that the data processing was in compliance with the data protection laws.

In the event of harm to personal rights caused to the data subject in connection with data processing or breach of data security requirements, the data subject may plead before the courts for the controller to cease and desist from infringement, for satisfaction, as well as for the perpetrator to hand over financial gains made from the infringement. Moreover, since 15 March 2014, the data subject may also claim exemplary damages – namely lump sum damages that can be awarded by the court for the compensation of the harm by the data controller as a result of unlawful data processing or breach of data security requirements. Regarding the claim for exemplary damages, the data subject as a claimant does not need to evidence the harm beyond the breach of data protection laws.

Penalties imposed by the DPA are made public via its website. The DPA has imposed penalties three times between 25 August and 31 December 2016, and seven times in 2017 up to 1 September. The maximum penalty of 20 million forints has not been imposed since September 2015; neither has the minimum amount of 100,000 forints. The amounts of imposed data protection fines since August 2016 have ranged from 300,000 to 8.5 million forints.

31 NAIH/2017/1051/2/H.
32 www.naih.hu.
VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The scope of the Hungarian Privacy Act covers all kinds of data controlling and processing regarding the data of private persons, data of public interest or data that is public because of the public interest. The Hungarian Privacy Act is also applied if a data controller handling personal data is located outside the European Union and it commissions a data controller with a seat, business establishment, branch office, domicile or place of residence in Hungary, or uses a device located in Hungary, except when this device serves only to transit data traffic in the area of the European Union. If the Privacy Act applies, a data controller shall appoint a representative for the territory of Hungary.

There are currently no requirements for the forced localisation of data servers, but it cannot be ruled out that the latest Russian developments (a recently enacted law creates a new obligation for data controllers to only store the personal data of Russian citizens within Russia) might influence the legal environment in Hungary.

The forwarding of personal data by an employer to a data processor located outside Hungary is not forbidden; however, it is subject to prior notification of the employee.

IX CYBERSECURITY AND DATA BREACHES

Hungary is a member of the Council of Europe's Convention on Cybercrime, which was signed in 2001 in Budapest. A government decision was issued recently in which the basics of the National Cybersecurity Strategy of Hungary were laid down. In connection with this legal development, a series of other laws has been announced covering areas such as the electronic information security of the state and local governments, and the responsibilities of the National Electronic Information Security Authority and the National Cybersecurity Coordination Council. Critical systems and facilities have also been identified, and their special protection has been ordered by law.

In Hungary, the obligation to make reports in line with the European Union Agency for Network and Information Security guidelines only extends to the organs of public administration. However, private persons can also contact the Government Incident Response Team by email or telephone.

X OUTLOOK

The EU General Data Protection Regulation was adopted on 27 April 2016, and will bring significant changes to the Hungarian data protection and privacy regime with effect from 25 May 2018. The Ministry of Justice prepared and submitted a bill of law to the Parliament in late August 2017 aiming to harmonise the Privacy Act with the upcoming new regime. In practical terms, the general and detailed debate on the bill will take place during the parliamentary session of autumn 2017, while the amendments are expected to enter into force in spring 2018.
Chapter 14

INDIA

Aditi Subramaniam and Sanuj Das

I OVERVIEW

A decidedly inadequate collection of statutes currently governs cybersecurity and data protection in India. Authorities constituted to regulate compliance and enforce penalties for non-compliance under the Information Technology Act 2000 and the Information Technology (Amendment) Act 2008 have been inactive for years, and very little significant jurisprudential development has occurred on the subjects of cybersecurity, privacy and data protection over the past few years. In 2013, the then government drafted a National Cybersecurity Policy, which generated considerable interest both in India as well as abroad, particularly in view of India’s position as an exponentially growing business process outsourcing destination. Sadly, progress on the policy was stymied for reasons that have not been made public, reflecting rather poorly on the government’s intention to provide clear, robust and watertight law on these matters.

The foregoing is not to say that the urgent need for change in this respect has not been recognised. At a national cybersecurity conference in New Delhi held in July 2016 under the patronage of the PHD Chamber of Commerce and Industry, the Joint Secretary for Cyber Laws and E-Security, R K Sudhanshu, stated to the press that the government is in the process of developing new encryption and cybersecurity policies as part of a thorough overhaul of the law regulating cybersecurity in India.2

Recently, the Minister for Law and IT, Ravi Shankar Prasad, while addressing an Associated Chambers of Commerce and Industry in India conference on network security and cybersecurity, said that the government is finalising cybersecurity standards for mobile phones and has already issued notice to most smartphone manufacturers asking them to furnish details related to cybersecurity.

Following the government launch, in 2015, of a heavily advertised campaign called Digital India, the major agenda of which was to create ‘digital infrastructure’ to facilitate the digital delivery of services and increase digital literacy, the prime minister has been involved in an aggressive attempt to compensate for lost time as regards the enhancement of cybersecurity. Digital India triggered major investment flows into the technology sector, and the campaign has caused questions to be raised in the media and academia about privacy and the protection of data, which will hopefully spur the government on to legislate more clearly and in detail on these subjects.

1 Aditi Subramaniam is a senior associate and Sanuj Das is an associate at Subramaniam & Associates.
Subsequently, 2016 was a mixed bag of both encouraging and slightly disturbing developments, although notably none of these developments resulted in the substantive renovation or repair of statutory law, as has been repeatedly promised by the authorities for several years, with the exception of the introduction of the Aadhar Act, to provide targeted delivery of financial benefits.

The Aadhar Act was challenged in a series of petitions that questioned its constitutional validity. A moot question raised in these petitions was whether privacy is a fundamental right guaranteed under the Constitution of India. The verdict on these petitions was delivered this year by a nine-judge constitutional bench of the Supreme Court, which held privacy to be a fundamental right of every citizen under the Constitution.3

In addition to the litigious developments described above, this year also saw the government amending the Income Tax Act 1961–2017 to make it mandatory for taxpayers to link their Permanent Account Numbers (PANs) to file income-tax returns, open bank accounts and conduct financial transactions beyond a threshold, to curb tax evasion and money laundering. The Department of Telecommunications has also mandatorily sought to use the Aadhar Act as a tool for subscriber verification from existing mobile telephone subscribers and made it mandatory for new connections.4 These developments are discussed in detail below.

II THE YEAR IN REVIEW

The following major developments of note occurred in the course of the past year, and these affect national policy, legislation and jurisprudence on cybersecurity, data protection and privacy to varying degrees.

i Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (the Aadhar Act)

The government pushed the Aadhar bill through parliament in a week in March 2016, resulting in the Aadhaar Act. Briefly, the Act provides for the issuance of an identification number issued by the Unique Identification Authority of India to citizens of the country. This number will be used to deliver state subsidies directly into the hands of beneficiaries.

The Aadhaar scheme was first mooted as the Indian equivalent to the social security number in the United States. The passage of this bill into law has, however, generated furious debate about the privacy concerns it necessarily raises – the Act envisages the creation of a database of personal identifying information of potentially a billion unsuspecting citizens, and also the use of the data therein to facilitate mass surveillance, and absolutely no framework or legislation is in place to regulate either the former or the latter. The Act contains provisions on the strict limitation on sharing the data collected, but also makes rather large exceptions to these limitations that are a major cause for concern.5

In a writ petition before the apex court of the country, the Aadhar Act was challenged as being ultra vires in relation to the Constitution owing to its severe violation of citizens’ fundamental right to privacy. It was put to the court that the Aadhar Act coerces individuals to

part with their personal information, including biometric details, and creates an environment that can be used for surveillance. While the fate of the Aadhar Act is still undecided, one of the biggest hurdles in the matter has been resolved by the Supreme Court in a landmark judgment. A nine-judge constitution bench, presided over by the Chief Justice of India, was posed the question of whether privacy is in fact a fundamental right guaranteed under the Constitution.

The Court ruled on this question in the affirmative and in doing so observed that it is not an absolute right but one subject to certain reasonable restrictions. On the data protection aspect, the Court observed that the right of an individual to exercise control over his or her personal data and to be able to control his or her own life would also encompass the right to control his or existence on the internet. The judgment also states that consent obtained from users has to be informed consent, given in an informed manner by users, and cannot be shrouded in lengthy agreement terms, The Court even upheld the right of an individual to be forgotten from the internet by observing that:

If we were to recognise a similar right, it would only mean that an individual who is no longer desirous of his personal data to be processed or stored, should be able to remove it from the system where the personal data/information is no longer necessary, relevant, or is incorrect and serves no legitimate interest. Such a right cannot be exercised where the information/data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy.

ii  WhatsApp litigation
In widely publicised litigation in the public interest against WhatsApp, the privacy policies of WhatsApp and Facebook were called into question. This case is discussed in more detail in Section VII.iii.

iii  US–India Cyber Relationship
In his final visit to the United States before the end of Barack Obama’s term as president, our Prime Minister Narendra Modi held significant discussions on cybersecurity cooperation with the president, resulting in the signing of the framework for the US–India Cyber Relationship. This bilateral framework will cover aspects of internet governance, cybersecurity and the building of norms of state behaviour.6

iv  India selected as a member of the UN group of governmental experts (GGE) to identify ‘rules of the road’ for cyberspace
India has been selected to be a member of the 2016 GGE set up to identify ‘rules of the road’ for cyberspace. While the GGE’s report is endorsed by the General Assembly, it is not officially binding. However, in combination with the initiation of the US–India Cyber Relationship, India’s participation in the 2016 GGE meeting signifies a way forward in the framing of issues that must be addressed in these matters.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

In the absence of specific legislation, data protection is achieved in India through the enforcement of privacy rights on the basis of a patchwork of legislation, as follows.

_The Information Technology Act (2000) (IT Act) and the Information Technology (Amendment) Act 2008_\(^7\)

The IT Act contains provisions for the protection of electronic data. The IT Act penalises ‘cyber contraventions’ (Section 43(a)–(h)), which attract civil prosecution, and ‘cyber offences’ (Sections 63–74), which attract criminal action.

The IT Act was originally passed to provide legal recognition for e-commerce and sanctions for computer misuse. However, it had no express provisions regarding data security. Breaches of data security could result in the prosecution of individuals who hacked into the system, under Sections 43 and 66 of the IT Act, but the Act did not provide other remedies such as, for instance, taking action against the organisation holding the data. Accordingly, the IT (Amendment) Act 2008 was passed, which, _inter alia_, incorporated two new sections into the IT Act, Section 43A and Section 72A, to provide a remedy to persons who have suffered or are likely to suffer a loss on account of their personal data not having been adequately protected.

_The Information Technology Rules (the IT Rules)_

Under various sections of the IT Act, the government routinely gives notice of sets of Information Technology Rules to broaden its scope. These IT Rules focus on and regulate specific areas of collection, transfer and processing of data, and include, most recently, the following:

\(a\) the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,\(^8\) which require entities holding users’ sensitive personal information to maintain certain specified security standards;

\(b\) the Information Technology (Intermediaries Guidelines) Rules,\(^9\) which prohibit content of a specific nature on the internet, and an intermediary, such as a website host, is required to block such content;

\(c\) the Information Technology (Guidelines for Cyber Cafe) Rules,\(^10\) which require cybercafes to register with a registration agency and maintain a log of users’ identities and their internet usage; and

\(d\) the Information Technology (Electronic Service Delivery) Rules,\(^11\) which allow the government to specify that certain services, such as applications, certificates and licences, be delivered electronically.

---

\(^7\) Links to PDF versions of the IT Act and Rules are available on the website of the Ministry of Electronics and Information Technology: meity.gov.in/content/cyber-laws.

\(^8\) meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.


The IT Rules are statutory law, and the four sets specified above were notified on 11 April 2011 under Section 43A of the IT Act.

Penalties for non-compliance are specified by Sections 43 and 72 of the IT Act.

In 2011 and subsequently in 2014, draft versions of a proposed law referred to as the Privacy Bill were released on the internet by a non-profit organisation called the Centre for Internet and Society, which claimed that these drafts had been leaked by the Department of Electronics and Information Technology. The Privacy Bill recognises an individual’s right to privacy, but states also that certain circumstances, including protection of national integrity or sovereignty, national security, prevention of crime and public order, warrant the invasion of that privacy. In May 2016, the Minister for Communications and Information Technology, Ravi Shankar Prasad, stated in the upper house of Parliament that the government is still working on the proposed law.

Additional legislation

In addition to the legislation described above, data protection may also sometimes occur through the enforcement of property rights based on the Copyright Act (1957). Further, other legislation such as the Code of Criminal Procedure (1973), the Indian Telegraph Act 1885, the Companies Act (1956), the Competition Act (2002) and, in cases of unfair trade practices, the Consumer Protection Act (1986), would also be relevant. Finally, citizens may also make use of the common law right to privacy, at least in theory – there is no significant, recent jurisprudence on this.

Compliance regulators

CERT-In

Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the ‘Indian Computer Emergency Response Team’. CERT-In is a national nodal agency responding to computer security incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

- collection, analysis and dissemination of information on cybersecurity incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- coordination of cybersecurity incident response activities; and
- issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity incidents.

Cyber Regulations Appellate Tribunal (CRAT)

Under Section 48(1) of the IT Act 2000, the Ministry of Electronics and Information Technology established CRAT in October 2006. The IT (Amendment) Act 2008 renamed the tribunal Cyber Appellate Tribunal (CAT). Pursuant to the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer

---

14 www.cert-in.org.in.

© 2017 Law Business Research Ltd
under this Act, may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.

Before the IT (Amendment) Act 2008, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise of a chairperson and such a number of other members as the central government may notify or appoint.15

**Definitions**

The legislation does not contain a definition of ‘personal data’. The IT Rules do define personal information as any information that relates to a natural person that, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.

Further, the IT Rules define ‘sensitive personal data or information’ as personal information consisting of information relating to:

- passwords;
- financial information, such as bank account, credit card, debit card or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information;
- any details relating to the above clauses as provided to a body corporate for the provision of services; or
- any information received under the above clauses by a body corporate for processing, or that has been stored or processed under lawful contract or otherwise.

Provided that any information is freely available or accessible in the public domain, or furnished under the Right to Information Act 2005 or any other law for the time being in force, it shall not be regarded as sensitive personal data or information for the purposes of these rules.

The Privacy Bill contains more specific definitions of the above terms, and also defines concepts not found in the current legislation, such as ‘processing’, ‘data controller’ and ‘data processor’.

**General obligations for data handlers**

**Obligations for data processors, controllers and handlers**

**Transparency**

The IT Rules state that all data handlers must create a privacy policy to govern the way they handle personal information. Further, the policy must be made available to the data subject who is providing this information under a lawful contract.

**Lawful basis for processing**

A body corporate (or any person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the data subject to use it for that specific purpose.

---

Consent must be obtained before collection of the data. The IT Rules also mandate that sensitive personal information may not be collected unless it is connected to the function of the corporate entity collecting it, and then only if the collection is necessary for that function. It is the responsibility of the body corporate to ensure that the sensitive personal information thus collected is used for no other purpose than the one specified.

**Purpose limitation**

Neither the IT Rules nor the IT Act specify a time frame for the retention of sensitive personal information. However, the IT Rules state that a body corporate or any person on its behalf holding sensitive personal data or information shall 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.

**Data retention**

Legislation is yet to be clarified on specific rules with respect to the retention of data by data processors or handlers.

**Registration formalities**

India currently does not have any legislative requirements with respect to registration or notification procedures for data controllers or processors. However, the draft Privacy Bill proposes to change this by introducing not only specific registration criteria and formalities, but also sanctions for failure of registration.

**Rights of individuals**

**Access to data**

Rule 5, Subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided.

**Correction and deletion**

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and to ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, Subsection 1 that corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

**Objection to processing and marketing**

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent that may have been given to the corporate entity previously, and the withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the corporate body is prohibited from processing the personal information in question. In the case of the data subject not providing consent, or later withdrawing consent, the corporate body shall have the option not to provide the goods or services for which the information was sought.
Disclosure of data

Data subjects also possess rights with respect to disclosure of the information they provide. Disclosure of sensitive personal information requires the provider’s prior permission unless either disclosure has already been agreed to in the contract between the data subject and the data controller; or disclosure is necessary for compliance with a legal obligation.

The exceptions to this rule are if an order under law has been made, or if a disclosure must be made to government agencies mandated under the law to obtain information for the purposes of verification of identity; prevention, detection and investigation of crime; or prosecution or punishment of offences.

Recipients of this sensitive personal information are prohibited from further disclosing the information.

iii Specific regulatory areas

Financial privacy

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983

Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except in accordance with laws of practice and usage.

The Prevention of Money Laundering Act 2002

The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offence under the PMLA.

Credit Information Companies (Regulation) Act 2005 and The Credit Information Companies Regulations 2006

This legislation is essentially aimed at regulation of sharing and exchanging credit information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offences is maintained permanently while information relating to civil offences is

retained for seven years from the first reporting of the offence. In fact, the regulations also prescribe that personal information that has become irrelevant may be destroyed, erased or made anonymous.

Credit information companies are required to obtain informed consent from individuals and entities before collecting their information. For the purpose of redressal, a complaint can be written to the Reserve Bank of India.

**Payment and Settlement Systems Act 2007**

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

**Foreign Contribution Regulation Act 2010**

This Act is aimed at regulating and prohibiting the acceptance and utilisation of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

**Workplace privacy**

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, in relation to the workplace, the effect of the Supreme Court judgment on privacy as a fundamental right remains to be seen.

**Children’s privacy**

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child’s best interest.

20  https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf.
**Health and medical privacy**

*Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)*

Under these regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

**Medical Termination of Pregnancy Act 1971**

This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

**Ethical Guidelines for Biomedical Research on Human Subjects**

These Guidelines require investigators to maintain confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person's life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is risk to public health.

**iv Technological innovation and privacy law**

There are no marketing restrictions on the internet or through email. Because India has no comprehensive data protection regime, issues such as cookie consent have not yet been addressed by Indian legislation.

The IT Rules provide reasonable security practices to follow as statutory security procedures for corporate entities that collect, handle and process data, and these also apply to the use of big data. Unfortunately, no specific guidelines exist for the use of big data and big-data analytics in India.

**IV INTERNATIONAL DATA TRANSFER**

Despite India’s dogged attempts to join the APEC for several years, its inclusion on the forum has so far been limited to observer status. APEC rules therefore do not apply in the Indian jurisdiction thus far.

In terms of restrictions on transfer of data, Section 7 of the IT Rules states that bodies corporate can transfer sensitive personal data to any other body corporate or person within or outside India, provided the transferee ensures the same level of data protection that the body corporate maintained, as required by the IT Rules. A data transfer is only allowed if it is required for the performance of a lawful contract between the data controller and the data subjects; or the data subjects have consented to the transfer.

The proposed Privacy Bill, if enacted, will place slightly more stringent restrictions on international transfers of personal data.

---

As worded, Section 7 is already rather restrictive. However, in some ways this is no different from EU data protection legislation, which restricts transfers of personal data outside the EU unless certain measures are taken, such as requiring the data importer to sign up to EU Model Contract Clauses. In addition, the Ministry of Information Technology clarified via a press note released on 24 August 2011 that the rules on sensitive data transfer described above are limited in jurisdiction to Indian bodies corporate and legal entities or persons, and do not apply to bodies corporate or legal entities abroad. As such, information technology industries and business process outsourcing companies may subscribe to whichever secure methods of data transfer they prefer, provided that the transfer in question does not violate any law either in India or in the country the data are being transferred to. Presumably litigation in this sector – so far non-existent – will further clarify matters.

V  COMPANY POLICIES AND PRACTICES

The general obligations for data handlers elaborated above apply to all companies handling data, and their policies must reflect as much. In addition, the IT Rules contain specific legislation to deal with best practices, particularly in the context of breach and security.

Rule 8 of the IT Rules describes reasonable security practices and procedures as follows:

1. A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have 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 with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall 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.


3. 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 as per sub-rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

4. The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall 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 entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.
VI DISCOVERY AND DISCLOSURE

If requests from foreign companies are based on an order from a court of law, and if the country in question has a reciprocal arrangement with India, then an Indian court is likely to enforce the request in India. In the absence of a court order, however, no obligation exists against an Indian company to make any kind of disclosure.

In a Ministry of Communications and Information Technology press release, the government clarified that any Indian outsourcing service provider or organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligations with a legal entity located within or outside India is not subject to the IT Rules requirements with respect to disclosure of information or consent, provided it does not have direct contact with the data subjects when providing services.

See also the exceptions to the consent requirements for disclosure detailed in Section III.ii.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

In addition to the security practices and policies outlined in Section V, and as mentioned in Section III.i, the proposed Privacy Bill conceptualises the creation of a data protection authority for the enforcement of data protection legislation and to oversee compliance with it. The Privacy Bill will override the IT Rules if it is enacted, and in that event, its provisions pertaining to the security of personal data that state specifically that every data controller must set appropriate technological, organisational and physical standards for the security of data under its control will also come into force.

ii Recent enforcement cases

As is evident from the above, India has no distinct legislative framework to support litigation in the areas of privacy, cybersecurity and data protection. There has been no significant litigation in this area in the recent past. It is to be hoped that with the passage of the Privacy Bill into law and a clearer definition of rights in this sector, the enforcement of rights will become both more active and more stringent.

iii Private litigation

Karmanya Singh Sareen & Anr v. UOI & Ors

This case was filed before the High Court of New Delhi in the public interest by two university students against WhatsApp, Facebook and the Union of India (through the Department of Telecommunications (DoT) and the Telecom Regulatory Authority of India (TRAI)). Subsequent to its acquisition by Facebook, WhatsApp updated its privacy policy in August 2016, stating that it would now share a limited amount of user information with Facebook for optimised advertising and networking suggestions. The petitioners contended that this change in policy compromised the privacy of the users of WhatsApp.

22 (WP(C) 7663/2016): lobis.nic.in/ddir/dhc/GRO/judgement/24-09-2016/GRO23092016CW76632016.pdf.
On 23 September 2016, the High Court of New Delhi passed an order directing WhatsApp to ‘scrub’ all user data collected prior to 25 September for users who chose to opt out of the service prior to this date. For users choosing to continue to make use of the service, the High Court directed that only data collected after 25 September could be shared by WhatsApp with Facebook and its group companies. The Court also directed DoT and TRAI to examine the feasibility of bringing WhatsApp (and other internet-based messaging applications) under a statutory regulatory framework, ordering that these respondents must take an appropriate decision on this matter ‘at the earliest’.

This decision is significant in that it is the only emphatic recognition of the right to privacy for individuals that our jurisprudence has seen in the past few years, other than the landmark Supreme Court judgment striking down Section 66A of the IT Act in 2015.

Earlier this year, the petitioners filed an appeal before the Supreme Court challenging the order of the High Court. The petitioners have impugned the directions of the High Court and seek directions of the Supreme Court since, according to the petitioners, the policy formulated by WhatsApp is unconscionable and unacceptable. The Supreme Court is still hearing the matter and it seems unlikely that the controversy will be resolved this year.

KS Puttaswamy & Ors v. Union of India & Ors

In KS Puttaswamy & Ors v. Union of India & Ors, and litigation that followed it, the constitutional validity of the Aadhar Act scheme was challenged on the grounds that it was *ultra vires* in relation to the constitution and violated the rights of every citizen.

The matter was initially heard by a three-judge bench, which referred it to a five-judge bench. However, owing to previous judgments by larger benches of the Supreme Court, a nine-judge bench was constituted to address the issue of whether privacy was a fundamental right guaranteed under the Constitution. The nine-judge bench gave a unanimous decision holding privacy to be a fundamental right of every citizen of the country, with qualified riders. In fact, the judgment acknowledges neo-libertarian values such as the right to be forgotten and will go down as a landmark judgment in the annals of legal history.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Unfortunately, Indian jurisprudence sheds no light on compliance requirements for organisations functioning outside the Indian jurisdiction (see Section IV for more details).

IX CYBERSECURITY AND DATA BREACHES

See Sections V and VI for information on breaches and breach reporting requirements. In addition to the information given in those sections, it is pertinent to note that in the context of a legal requirement to report data breaches to individuals, while the law as it is contains no such provision, the draft Privacy Bill does. In fact, the draft exempts the data protection authority from this requirement in only two scenarios: if the data protection authority believes that such a notification will impede a criminal investigation or the identity of the data subject cannot possibly be identified.

---

X OUTLOOK

There is no doubt that India sorely needs to take a keen look at its poorly regulated digital spaces and at the virtual activities of individuals, private organisations and governmental authorities alike. The several agencies performing cybersecurity operations in India, such as the National Technical Research Organisation, the National Intelligence Grid and the National Information Board, require robust policy and legislative and infrastructural support from the Ministry of Electronics and Information Technology, and from the courts, to enable them to do their jobs properly. The EU’s data protection regulation may provide impetus for India in this regard, particularly given that not only will the regulation affect cross-border information flow (and India is a net information exporter), but also the EU has exposed several lacunae in the standards applied by the Indian government to the protection of data and enforcement of cybersecurity in a report following approval of its new data protection regulation. TRAI has recently released a consultation paper titled ‘Privacy, Security and Ownership of the Data in the Telecom Sector’, inviting comments from concerned stakeholders for issues faced regarding data privacy and security in the telecom sector. While it seems that the government is concerned and keen to bring about change in this sector, in view of India’s rather poor record in prioritising these matters, optimism is not necessarily warranted at this stage.
I OVERVIEW

In Japan, the Act on the Protection of Personal Information (APPI) primarily handles the protection of data privacy issues. The APPI was drastically amended in 2016 and has been in full force since 30 May 2017. Prior to the amendment, the APPI was applied solely to business operators that have used any personal information database containing details of more than 5,000 persons on any day in the past six months but this requirement was eliminated by the amendment. Under the amended APPI, the Personal Information Protection Commission (PPC) was established as an independent agency whose duties include protecting the rights and interests of individuals while promoting proper and effective use of personal information. Under the amended APPI, the legal framework has been drastically changed and the PPC has primary responsibility for personal information protection policy in Japan. Prior to the amendment, as of July 2015, 39 guidelines for 27 sectors regarding personal information protection were issued by government agencies, including the Ministry of Health, Labour and Welfare, the Japan Financial Services Agency, and the Ministry of Economy, Trade and Industry. Under the amended APPI, however, the guidelines (the APPI Guidelines) that prescribe in detail the interpretations and practices of the APPI are principally provided by the PPC, with a limited number of special guidelines provided to specific sectors (such as medical and financial ones) by the PPC and the relevant ministries.

1 Tomoki Ishiara is an associate at Sidley Austin Nishikawa Foreign Law Joint Enterprise.
II THE YEAR IN REVIEW

i Background of the amendment to the APPI: Policy Outline of the Institutional Revision for Use of Personal Data (the Policy Outline), and the amendment to the APPI

On 24 June 2014, the government 9 published the Policy Outline, 10 showing the government’s direction on the measures to be taken to amend the APPI and the other personal information protection-related laws. The revision bill of the APPI passed the Diet on 3 September 2015 and the amended APPI has been in full force since 30 May 2017. The main changes introduced by the amendment to the APPI are set out below.

**Development of a third-party authority system**

The government has established an independent agency to serve as a data protection authority to operate ordinances and self-regulation in the private sector to promote the use of personal data. The primary amendments to the previous legal framework are as follows:

a the government has established the structure of the third-party authority ensuring international consistency, so that legal requirements and self-regulation in the private sector are effectively enforced;

b the government has restructured the Specific Personal Information Protection Commission prescribed in the Number Use Act 12 to set up the PPC, the new authority mentioned at (a), for the purpose of promoting a balance between the protection of personal data and effective use of personal data; and

c the third-party authority has the following functions and powers: 13

- formulation and promotion of basic policy for personal information protection;
- supervision;
- mediation of complaints;
- assessment of specific personal information protection;
- public relations and promotion;
- accreditation of private organisations that process complaints about business operators handling personal information and provide necessary information to such business operators, based on the amended Act on the Protection of Personal Information;
- survey and research the operations stated above at (c); and
- cooperation with data protection authorities in foreign states.

---

9 Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society.
11 The European Commission pointed out the lack of a data protection authority in the Japanese system in its report: Korfe, Brown, et al., ‘Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments’ (20 January 2010).
12 Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013). See Section II.i.
13 Article 61 APPI.
**Actions for globalisation**

If businesses handling personal data are planning to provide personal data (including personal data provided by overseas businesses and others) to overseas businesses, they have to obtain consent to the transfer from the principal except where:

- **a** no consent is necessary in accordance with the following exceptions to Article 23(1):[^1]
  - cases based on laws and regulations;
  - cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal’s consent;
  - cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal’s consent; and
  - cases in which there is a need to cooperate with a central government organisation or a local government, or a person entrusted by them acting in matters prescribed by laws and regulations, and when there is a possibility that obtaining a principal’s consent would interfere with the execution of these duties;

- **b** the overseas businesses establish a system conforming to operating standards prescribed by the PPC rules for overseas businesses to deal with personal information in a manner equivalent to that of a business operator handling personal data pursuant to the provisions of the APPI; and

- **c** the foreign countries in which the overseas businesses are conducted are prescribed by the PPC rules as having established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual’s rights and interests.

**Framework for promoting the use of personal data (big data issues)**

The use of personal data is expected to create innovation with the multidisciplinary utilisation of diverse and vast amounts of data, thereby creating new businesses. However, the system under the previous APPI required consent from principals to use their personal data for purposes other than those specified. Accordingly, providing personal data to third parties was cumbersome for businesses, and created a barrier to the use of personal data, especially launching new business using big data. Under the amended APPI, a business operator handling personal information may produce anonymously processed information (limited to information constituting anonymously processed information databases, etc.) and process personal information in accordance with standards prescribed by the PPC rules such that it is impossible to identify a specific individual from, or de-anonymise, the personal information used for the production.[^15] This amendment allows various businesses to share with other businesses the personal data maintained by them, and so develop or foster new business or innovation.

**Sensitive personal information**

The previous APPI did not define ‘sensitive personal information’; however, the amended APPI has defined information regarding an individual’s race, creed, social status, criminal record and past record as ‘special-care-required personal information’ (sensitive personal information),

[^1]: Article 23 APPI.
[^15]: Article 36(1) APPI.
along with any other information that may be the focus of social discrimination.\textsuperscript{16} Also, there was no provision that specifically addressed consent requirements for sensitive personal information in the previous APPI; instead these were regulated by a number of guidelines issued by government ministries. The amended APPI, however, explicitly requires that a business operator handling personal information obtain prior consent to acquire sensitive personal information, with certain exceptions.\textsuperscript{17}

In addition, the opt-out exception provided under Article 23 does not apply to sensitive personal information and consent to provide such information to third parties is required.\textsuperscript{18} The Policy Outline also mentions that in view of the actual use of personal information, including sensitive information, and the purpose of the current law, the government will lay down regulations regarding the handling of personal information, such as providing exceptions where required by laws and ordinances and for the protection of human life, health or assets, as well as enabling personal information to be obtained and handled with the consent of the persons concerned.

\textit{Enhancement of the protection of personal information: tractability of obtained personal information}

The amended revised APPI:

\begin{itemize}
  \item imposes obligations on business operators handling personal information to make and keep accurate records for a certain period when they provide third parties with personal information;\textsuperscript{19}
  \item imposes obligations on business operators handling personal information to verify third parties’ names and how they obtained personal information upon receipt of personal information from those third parties;\textsuperscript{20} and
  \item establishes criminal liability for providing or stealing personal information with a view to making illegal profits.\textsuperscript{21}
\end{itemize}

\textbf{ii} \textbf{Social security numbers}

The bill on the use of numbers to identify specific individuals in administrative procedures (the Number Use Act, also called the Social Security and Tax Number Act) was enacted on 13 May 2013,\textsuperscript{22} and provides for the implementation of a national numbering system for social security and taxation purposes. The government will adopt the social security and tax number system to enhance social security for people who truly need it; to achieve the fair distribution of burdens such as income tax payments; and to develop efficient administration. The former independent supervisory authority called the Specific Personal Information Protection Commission was transformed into the PPC, which was established on 1 January 2016 to handle matters with respect to both the Number Use Act and the

\begin{footnotesize}
\begin{enumerate}
  \item Article 1(3) APPI.
  \item Article 17(2) APPI.
  \item Article 23(2) APPI.
  \item Article 25 APPI.
  \item Article 26 APPI.
  \item Article 83 APPI.
  \item The revision bill of the Number Use Act was passed on 3 September 2015. The purpose of this revision was to provide further uses for the numbering system (e.g., management of personal medical history).
\end{enumerate}
\end{footnotesize}
amended APPI. This authority consists of one chair and eight commission members. The chair and commissioners were appointed by Japan's prime minister and confirmed by the National Diet. The numbering system fully came into effect on 1 January 2016. Unlike other national ID numbering systems, Japan has not set up a centralised database for the numbers because of concerns about data breaches and privacy.

iii Online direct marketing
Under the Act on Regulation of Transmission of Specified Electronic Mail and the Act on Specified Commercial Transactions, businesses are generally required to provide recipients with an opt-in mechanism, namely to obtain prior consent from each recipient for any marketing messages sent by electronic means. A violation of the opt-in obligation may result in imprisonment, a fine, or both.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Definitions

Personal information

The amended APPI clarifies the scope of ‘personal information’ as follows:

a information about a living person that can identify him or her by name, date of birth or other description contained in the information (including information that will allow easy reference to other information that will enable the identification of the specific individual), or

b information about a living person that contains an individual identification code, which means any character, letter, number, symbol or other codes designated by Cabinet Order, falling under any of the following items:

• those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily or partial feature of the specific individual has been converted to be provided for use by computers; and
• those characters, letters, numbers, symbols or other codes assigned in relation to the use of services provided to an individual, or to the purchase of goods sold to an individual, or that are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or stated or recoded for the said user or purchaser, or recipient of issuance.

[References]

24 Act No. 26 of 17 April 2002.
26 Article 2(1)(i) APPI.
27 Article 2(1)(ii), Article 2(2) APPI.
28 For example, according to the Cabinet Order, the information on sequences of bases of DNA, fingerprints, facial recognition (Article 2(2)(i)) and the information on driver licence, passport and insurance policy number (Article 2(2)(ii)) are regarded as an individual identification code.
**Personal information database**

A ‘personal information database’\(^{29}\) is an assembly of information including:

\(a\) information systematically arranged in such a way that specific personal information can be retrieved by a computer; or

\(b\) in addition, an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved.

**Business operator handling personal information**

A ‘business operator handling personal information’\(^{30}\) is a business operator using a personal information database, etc. for its business.\(^{31}\) However, the following entities shall be excluded:

\(a\) state organs;

\(b\) local governments;

\(c\) incorporated administrative agencies, etc.;\(^{32}\) and

\(d\) local incorporated administrative institutions.\(^{33}\)

**Personal data\(^{34}\)**

‘Personal data’ comprises personal information constituting a personal information database, etc. (when personal information such as names and addresses is compiled as a database, it is personal data in terms of the APPI).

**Sensitive personal information**

The previous APPI did not have a definition of ‘sensitive personal information’. However, for example, the Japan Financial Services Agency’s Guidelines for Personal Information Protection in the Financial Field (the JFSA Guidelines)\(^{35}\) have defined information related to political opinion, religious belief (religion, philosophy, creed), participation in a trade union, race, nationality, family origin, legal domicile, medical care, sexual life and criminal record as sensitive information.\(^{36}\) Furthermore, the JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,\(^{37}\) although some exceptions exist. Following these practices, the amended APPI has explicitly provided a definition of ‘sensitive personal information’ and its special treatment (see Section II.i).

---

\(^{29}\) Article 2(4) APPI.

\(^{30}\) Article 2(5) APPI.

\(^{31}\) As mentioned in Section I, the amended APPI applies to business operators that use any personal information database, regardless of the number of principals of personal information. Prior to the amendment, the APPI was applied solely to any personal information database containing details of more than 5,000 persons on any day in the past six months. See footnote 3.

\(^{32}\) Meaning independent administrative agencies as provided in Paragraph (1) of Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003).

\(^{33}\) Meaning local incorporated administrative agencies as provided in Paragraph (1) of Article 2 of the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003).

\(^{34}\) Article 2(6) APPI.


\(^{36}\) Article 6(1) of the JFSA Guidelines.

\(^{37}\) Article 6(1)1–8 of the JFSA Guidelines.
ii General obligations for data handlers

Purpose of use

Pursuant to Article 15(1) APPI, a business operator handling personal information must as far as possible specify the purpose of that use. In this regard, the Basic Policy on the Protection of Personal Information (Basic Policy) (Cabinet Decision of 2 April 2004) prescribes as follows:

To maintain society’s trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so-called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy-to-understand manner, their procedures relating to the handling of personal information, such as notification and announcement of the purpose of use and disclosure, etc., as well as comply with the relevant laws and ordinances.

The government formulated the Basic Policy based on Article 7, Paragraph 1 APPI. To provide for the complete protection of personal information, the Basic Policy shows the orientation of measures to be taken by local public bodies and other organisations, such as businesses that handle personal information, as well as the basic direction concerning the promotion of measures for the protection of personal information and the establishment of measures to be taken by the state. The Basic Policy requires a wide range of government and private entities to take specific measures for the protection of personal information.

In this respect, under the previous APPI, a business operator handling personal information could not change the use of personal information ‘beyond a reasonable extent’. The purpose of use after the change therefore had to be duly related to that before the change. The amended APPI has slightly expanded the scope of altering the purpose of use to enable flexible operations by prohibiting alteration of the utilisation purpose ‘beyond the scope recognised reasonably relevant to the pre-altered utilisation purpose’.38

In addition, a business operator handling personal information must not handle personal information about a person beyond the scope necessary for the achievement of the purpose of use, without obtaining the prior consent of the person.39

Proper acquisition of personal information and notification of purpose

A business operator handling personal information shall not acquire personal information by deception or other wrongful means.40

Having acquired personal information, a business operator handling personal information must also promptly notify the data subject of the purpose of use of that information or publicly announce the purpose of use, except in cases in which the purpose of use has already been publicly announced.41

38 Article 15(2) APPI.
39 Article 16(1) APPI.
40 Article 17 APPI.
41 Article 18(1) APPI.
Maintenance of the accuracy of data and supervision of employees or outsourcing contractors

A business operator handling personal information must endeavour to keep any personal data it holds accurate and up to date within the scope necessary for the achievement of the purpose of use. Under the amended APPI, a business operator handling personal information also must endeavour to delete personal data without delay when it becomes unnecessary.

In addition, when a business operator handling personal information has an employee handle personal data, it must exercise necessary and appropriate supervision over the employee to ensure the secure control of the personal data.

When a business operator handling personal information entrusts another individual or business operator with the handling of personal data in whole or in part, it shall also exercise necessary and appropriate supervision over the outsourcing contractor to ensure the secure control of the entrusted personal data.

Restrictions on provision to a third party

In general, a business operator handling personal information must not provide personal data to a third party without obtaining the prior consent of the data subject.

The principal exceptions to this restriction are as follows:

a. where the provision of personal data is required by laws and regulations;

b. where a business operator handling personal information agrees, at the request of the subject, to discontinue providing such personal data as will lead to the identification of that person, and where the business operator, in advance, notifies the PPC and the person of the following or makes this information readily available to the person in accordance with the rules set by the PPC:

• the fact that the provision to a third party is the purpose of use;
• which items of personal data will be provided to a third party;
• the method of provision to a third party;
• the fact that the provision of such personal data as might lead to the identification of the person to a third party will be discontinued at the request of the person; and
• the method of receiving the request of the person.

42 Article 19 APPI.
43 Article 21 APPI. For example, during training sessions and monitoring, whether employees comply with internal rules regarding personal information protection.
44 Article 22 APPI. The APPI Guidelines point out: (1) a business operator handling personal information has to prepare rules on the specific handling of personal data to avoid unlawful disclosure and maintain the security of personal data; and (2) a business operator handling personal information has to take systemic security measures (e.g., coordinate an organisation’s operations with regard to the rules on the handling of personal data, implement measures to confirm the treatment status of personal data, arrange a system responding to unlawful disclosure of personal data and review the implementation or improvement of security measures).
45 Article 23(1) APPI.
46 Article 23(1)(i) APPI. The APPI Guidelines mention the following cases:

a. response to a criminal investigation in accordance with Article 197(2) of the Criminal Procedure Law;

b. response to an investigation based upon a warrant issued by the court in accordance with Article 218 of the Criminal Procedure Law; and

c. response to an inspection conducted by the tax authority.
47 Article 23(2) APPI.
c where a business operator handling personal information outsources the handling of personal data (e.g., to service providers), in whole or in part, to a third party within the scope necessary for the achievement of the purpose of use;\(^{48}\)

d where personal information is provided as a result of the takeover of business in a merger or other similar transaction;\(^{49}\) and

e where personal data is used jointly between specific individuals or entities and where the following are notified in advance to the person or put in a readily accessible condition for the person:

- the facts;
- the items of the personal data used jointly;
- the scope of the joint users;
- the purpose for which the personal data is used by them; and
- the name of the individual or entity responsible for the management of the personal data concerned.\(^{50}\)

Public announcement of matters concerning retained personal data

Pursuant to Article 24(1) APPI, a business operator handling personal information must put the name of the business operator handling personal information and the purpose of use of all retained personal data in an accessible condition for the person concerned (this condition of accessibility includes cases in which a response is made without delay upon the request of the person), the procedures for responding to a request for disclosure, correction and cessation of the retention of the personal data.\(^{51}\)

Correction

When a business operator handling personal information is requested by a person to correct, add or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data are incorrect, the business operator must make an investigation without delay within the scope necessary for the achievement of the purpose of use and, on the basis of the results, correct, add or delete the retained personal data, except in cases where special procedures are prescribed by any other laws and regulations for such correction, addition or deletion.\(^{52}\)

IV INTERNATIONAL DATA TRANSFER

i Extraterritorial application of the APPI

It was generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI would be applicable to the entity

---

48 Article 23(5)(i) APPI.
49 Article 23(5)(ii) APPI.
50 Article 23(5)(iii) APPI.
51 The APPI Guidelines provide examples of what corresponds to such an accessible condition for the person, such as posting on the website, distributing brochures, replying without delay to a request by the person and providing the email address for enquiries in online electronic commerce.
52 Article 29(1) APPI.
handling personal information in Japan. In accordance with this accepted understanding, the amended APPI explicitly provides that the APPI applies to a business operator located outside Japan under certain circumstances.

The provisions of Article 15, Article 16, Article 18 (excluding Paragraph (2)), Articles 19 to 25, Articles 27 to 36, Article 41, Article 42 Paragraph (1), Article 43 and Article 76 apply in those cases where, in relation to provision of a good or service to a person in Japan, a business operator handling personal information has acquired personal information relating to that person and handles the personal information or anonymously processed information produced using the said personal information in a foreign country.53

ii International data transfers
With some exceptions prescribed in the APPI (see Section III.ii, ‘Restrictions on provision to a third party’), prior consent is required for the transfer of personal information to a third party.54 However, there was no specific provision regarding international data transfers in the previous APPI. To deal with the globalisation of data transfers, the amended APPI requires the consent of the principal to international transfers of personal data except in the following cases:55

a international personal data transfer to a third party (in a foreign country) that has established a system conforming to the standards set by the PPC rules56 (i.e., proper and reasonable measures taken in accordance with the provisions of the APPI or accreditation as a receiver of personal data according to international standards on the protection of personal information, such as being certified under the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules) for operating in a manner equivalent to that of a business operator handling personal data; and

b international personal data transfer to a third party in a foreign country that is considered, according to the rules of the PPC, to have established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual’s rights and interests.57

V COMPANY POLICIES AND PRACTICES
i Security control measures
A business operator handling personal information must take necessary and proper measures for the prevention of leakage, loss or damage of the personal data.58 Control measures may be systemic, human, physical or technical. Examples of these are listed below.

53 Article 75 APPI.
54 Article 23(1) APPI.
55 Article 24 APPI.
56 Article 11 Rules of the PPC.
57 At the time of writing, the PPC has not yet designated any country as having standards equivalent to those in Japan regarding the protection of personal information.
58 Article 20 APPI.
**Systemic security control measures**

- Preparing the organisation's structure to take security control measures for personal data;
- preparing the regulations and procedure manuals that provide security control measures for personal data, and operating in accordance with the regulations and procedure manuals;
- preparing the means by which the status of handling personal data can be looked through;
- assessing, reviewing and improving the security control measures for personal data; and
- responding to data security incidents or violations.

**Human security control measures**

- Concluding a non-disclosure agreement with workers when signing the employment contract and concluding a non-disclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of a temporary labourer); and
- familiarising workers with internal regulations and procedures through education and training.

**Physical security control measures**

- Implementing controls on entering and leaving a building or room where appropriate;
- preventing theft, etc.; and
- physically protecting equipment and devices.

**Technical security control measures**

- Identification and authentication for access to personal data;
- control of access to personal data;
- management of the authority to access personal data;
- recording access to personal data;
- countermeasures preventing unauthorised software on an information system handling personal data;
- measures when transferring and transmitting personal data;
- measures when confirming the operation of information systems handling personal data; and
- monitoring information systems that handle personal data.

**VI DISCOVERY AND DISCLOSURE**

**E-discovery**

Japan does not have an e-discovery system equivalent to that in the United States. Electronic data that include personal information can be subjected to a judicial order of disclosure by a Japanese court during litigation.

---

59 8-3 (Systemic Security Control Measures) of the APPI Guidelines, p. 88.
60 8-4 (Human Security Control Measures) and 3-3-3 (Supervision of Employees) of the APPI Guidelines, pp. 92, 41.
61 8-5 (Physical Security Control Measures) of the APPI Guidelines, p. 93.
62 8-6 (Technical Security Control Measures) of the APPI Guidelines, p. 96.
Disclosure
When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person, the business operator must disclose the retained personal data without delay by a method prescribed by a Cabinet Order. 63 However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed: 64

a where disclosure is likely to harm the life, person, property, or other rights or interests of the person or a third party;
b where disclosure is likely to seriously impede the proper execution of the business of the business operator handling the personal information; or
c where disclosure violates other laws and regulations.

VII PUBLIC AND PRIVATE ENFORCEMENT

Enforcement and sanctions

Enforcement agencies
Prior to the amendment, the enforcement agencies in data protection matters were the Consumer Affairs Agency, and ministries and agencies concerned with jurisdiction over the business of the relevant entities. Under the amended APPI, the PPC is the sole enforcement authority and it may transfer its authorities to request for report and to inspect to ministries and agencies if necessary for effective recommendations and orders under Article 42. 65

Main penalties 66
A business operator that violates orders issued under Paragraphs 2 or 3 of Article 42 (recommendations and orders by the PPC in the event of a data security breach) shall be sentenced to imprisonment with forced labour of not more than six months or to a fine of not more than ¥300,000. 67

A business operator that does not make a report 68 as required by Articles 40 or 56 or that has made a false report shall be sentenced to a fine of not more than ¥300,000. 69

63 The method specified by a Cabinet Order under Article 28(2) APPI shall be the provision of documents (or ‘the method agreed upon by the person requesting disclosure, if any’). Alternatively, according to the APPI Guidelines, if the person who made a request for disclosure did not specify a method or make any specific objections, then they may be deemed to have agreed to whatever method the disclosing entity employs.
64 Article 28(2) APPI.
65 Article 44 APPI.
66 The Unfair Competition Prevention Act (Act No. 47 of 1993) prohibits certain acts (unfair competition), including an act to acquire a trade secret from the holder by theft, fraud or other wrongful methods; and an act to use or disclose the trade secret so acquired. For the prevention of unfair competition, the Act provides measures, such as injunctions, claims for damages and penal provisions (imprisonment for a term not exceeding 10 years or a fine in an amount not exceeding ¥20 million. In the case of a juridical person, a fine not exceeding ¥1 billion (in certain cases the fine is not to exceed ¥500 million) may be imposed (Articles 21 and 22)).
67 Article 84 APPI.
68 The PPC may have a business operator handling personal information make a report on the handling of personal information to the extent necessary for fulfilling the duties of a business operator (Articles 40 and 56 APPI).
69 Article 85 APPI.
Recent enforcement cases

Information breach at a computer company

An outsourcing contractor of a computer company had their customer information acquired by a criminal following an illegal intrusion into the company’s network system. In May 2011, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the computer company reform its security control measures, supervision of outsourcing contractors, and training for outsourcing contractors and employees (in respect of violation of the duty regarding supervision of an outsourcing contractor under Article 22 APPI).70

Information breach at a mobile phone company

The email addresses of a mobile phone company were reset and email addresses of the customers and the mail texts were disclosed to third parties. In January 2012, the Ministry of Internal Affairs and Communications (MIC) promulgated an administrative guidance requesting that the mobile phone company take the necessary measures to prevent a recurrence and to report the result to the Ministry (in respect of violation of the duty regarding security control measures under Article 20 APPI).72

Information theft from mobile phone companies

The manager and employees of an outsourcing contractor of three mobile phone companies acquired customer information from the mobile phone companies unlawfully through their customer information management system and disclosed the customer information to a third party. In November 2012, the MIC introduced an administrative guidance requesting that the mobile phone companies reform their security control measures, supervision of outsourcing contractors, and training for outsourcing contractors and employees (in respect of violation of the duty regarding security control measures under Article 20 APPI and Article 11 of the MIC Guideline on Protection of Personal Information in Telecommunications.73 There was also found to be a violation of the duty regarding the supervision of outsourcing contractors under Article 22 APPI and Article 12 of the above-mentioned MIC Guideline).74

Information theft from a mobile phone company

In July 2012, a former store manager of an agent company of a mobile phone company was arrested for disclosing customer information of the mobile phone company to a research company (in respect of violation of the Unfair Competition Prevention Act). The Nagoya District Court in November 2012 gave the defendant a sentence of one year and eight months’ imprisonment with a four-year stay of execution and a fine of ¥1 million.75

70 3-3-4 of the APPI Guidelines, p.42.
71 3-3-2 of the APPI Guidelines, p. 41.
73 Announcement No. 695 of 31 August 2004 by the MIC.
Information theft from an educational company

In July 2014, it was revealed that the customer information of an educational company (Benesse Corporation) had been stolen and sold to third parties by employees of an outsourcing contractor of the educational company. In September 2014, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the educational company reform its security control measures and supervision of outsourcing contractors (in respect of violation of the duty regarding security control measures under Article 20 APPI). There was also found to be a violation of the duty regarding the supervision of an outsourcing contractor under Article 22 APPI. Benesse Corporation actually distributed a premium ticket (with a value of ¥500) to its customers to compensate for the damage incurred by the customers. Currently, however, a lawsuit is pending before the Supreme Court brought by a customer requesting damages of ¥100,000 (Osaka High Court dismissed the customer’s claim). It is anticipated that the Supreme Court will deliver an opinion clarifying the liability of businesses handling personal information and the calculation of damages due to a person as a result of the leaking of that person’s personal information.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As stated in Section IV, it is generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI is applicable to the entity handling personal information in Japan. The amended APPI requires that business operators obtain consent from the principal for international transfers of personal data. However, foreign business operators may circumvent this restriction by implementing proper and reasonable measures to protect personal information in accordance with the standards provided by the APPI.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The amendments to the Criminal Code, effective since 14 July 2011, were enacted to prevent and prosecute cybercrimes. Since under the previous law it was difficult to prosecute a person who merely stored a computer virus in his or her computer for the purpose of providing or distributing it to the computers of others, a person who not only actively creates, provides or distributes a computer virus, but also who acquires or stores a computer virus for the purpose of providing or distributing it to the computers of others without justification, may not be held criminally liable under the amendments.

Following the 2011 amendments, three primary types of behaviours are considered as cybercrimes: the creation or provision of a computer virus; the release of a computer virus; and the acquisition or storage of a computer virus. The Act on the Prohibition of Unauthorised Computer Access (APUCA) was also amended on 31 March 2012 and took effect in May of that year. The APUCA identified additional criminal activities, such as the

76 Act No. 45 of 1907, Amendment: Act No. 74 of 2011.
unlawful acquisition of a data subject’s user ID or password for the purpose of unauthorised computer access, and the provision of a data subject’s user ID or password to a third party without justification.

Following a 2004 review, the government has begun developing essential functions and frameworks aimed at addressing information security issues. For example, the National Information Security Centre was established on 25 April 2005, and the Information Security Policy Council was established under the aegis of an IT Strategic Headquarters (itself part of the Cabinet) on 30 May 2005.

Finally, the Basic Act on Cybersecurity, which provides the fundamental framework of cybersecurity policy in Japan, was passed in 2014.

ii Data security breach

There is no express provision in the APPI creating an obligation to notify data subjects or data authorities in the event of a data security breach. However, the APPI Guidelines stipulate that actions to be taken in response to data breach, etc. should be described separately from the Guidelines. The PPC has set out desirable actions as follows:

\[\begin{align*}
\text{a} & \quad \text{internal report on the data breach, etc. and measures to prevent expansion of the damage;} \\
\text{b} & \quad \text{investigation into any cause of the data breach, etc.;} \\
\text{c} & \quad \text{confirmation of the scope of those affected by the data breach, etc.;} \\
\text{d} & \quad \text{consideration and implementation of preventive measures;} \\
\text{e} & \quad \text{notifications to any person (to whom the personal information belongs) affected by the data breach etc.;} \\
\text{f} & \quad \text{prompt public announcement of the facts of the data breach, etc. and preventive measures to be taken; and} \\
\text{g} & \quad \text{prompt notifications to the PPC about the facts of the data breach, etc. and preventive measures to be taken except for where the data breach, etc. has caused no actual, or only minor, harm (e.g., wrong transmissions of facsimiles or emails that do not include personal data other than names of senders and receivers).}
\end{align*}\]

In addition, the PPC has the authority to collect reports from, or advise, instruct or give orders to, the data controllers.

An organisation that is involved in a data breach may, depending on the circumstances, be subject to the suspension, closure or cancellation of the whole or part of its business operations, an administrative fine, penalty or sanction, civil actions and class actions or a criminal prosecution.

---

78 Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues (IT Strategic Headquarters, 7 December 2004).


80 Act No. 104 of 12 November 2014.

81 PPC Announcement No.1 of 2017.

82 Articles 40–42 APPI.
X OUTLOOK

i The future development of the amended APPI
As stated in Section II, the amended APPI, which entered fully into force in May 2017, has drastically changed the legal framework for the protection of personal information in Japan. As of this writing, there have as yet been no leading cases or new matters to which the amended APPI applies and, led by the PPC, new practices based upon the new framework have just started. It is anticipated that the role of the PPC will be central to the new privacy policy in Japan and thus special attention should be paid to its activities for insight into the future development of the amended APPI.

ii The judicial reaction to the leaking of personal information in Japan
As stated in Section VII, an important data breach case (Benesse Corporation) is currently pending before the Supreme Court and its decision may articulate the scope of the obligations of business operators handling personal information and the calculation of damages arising from data breaches in Japan.
I OVERVIEW

Under the Constitution of Korea, the right to privacy is recognised as being a fundamental right and the right to control one’s personal information is regarded as having derived mainly from this right to privacy. In addition, the Constitutional Court of Korea established the right to control one’s personal information as a separate fundamental right independent from the right to privacy or other fundamental rights. The Constitutional Court of Korea defined the right to control personal information as the individual’s right to control the disclosure and use of his or her personal information. The specific rights associated with this right to control personal information are considered to be:

a. the right to prevent the collection and usage of personal information in the absence of the data subject’s prior consent;
b. the right to access and request correction of collected personal information;
c. the right to request suspension of the collection and usage of personal information; and
d. the right to request destruction of stored personal information, etc.

The system of individual laws related to the protection of personal information is primarily based on the detailed rights related to the fundamental right to control one’s personal information in specific industries or businesses.

The framework act for the protection of personal data in Korea is the Personal Information Protection Act (PIPA), which regulates collection, usage, disclosure and other processing (collectively, processing or process) of personal information by governmental and private entities. In addition to the PIPA, the processing of personal information by online service providers, including telecommunication service providers, is regulated by the Act on Promotion of Information Communication Network Usage and Information Protection (the Network Act), and the processing of (personal) credit information by financial institutions is regulated by the Act on Usage and Protection of Credit Information (the Credit Information Act). For the processing of personal information by online service providers and the processing of credit information by financial institutions, the Network Act and the Credit Information Act will each be applied ahead of the PIPA.

Although the PIPA imposes general cybersecurity requirements on data handlers (defined below), because of the nature of cybersecurity, the requirements for online service providers under the Network Act are considered to be more important. Financial institutions are subject to the cybersecurity requirements under the Credit Information Act as well as

---

1 Kwang Bae Park and Ju Bong Jang are partners at Lee & Ko.
Korea is known to have one of the strictest data protection regulatory regimes in the world. Because the processing of personal data by governmental and private entities is contingent on the express opt-in consent of the data subject (with limited exceptions for private entities and wider exceptions for governments), business activities or industries that require extensive processing of personal data, such as online target marketing or the big data industry, are less developed in Korea compared with its well-established IT infrastructure, and the role of self-regulatory industry groups is expanding but still quite limited. Because of these circumstances, criticism from affected industries and practitioners regarding the strict regulation of personal data processing is increasing, and regulators are becoming more sympathetic to some of this criticism. As a result, regulatory guidance in the form of the Guidelines for De-Identification of Personal Information (the Guidelines) was announced on 30 June 2016 to promote the development of industries using data and legislators are attempting to reform the regulatory system to reflect developments in the IT industry. Although the balance between the right to privacy and freedom of expression has not been a widely discussed issue in Korea, the situation could change in the near future in light of the current debate concerning the ‘right to be forgotten’.

Because the Credit Information Act and other laws tend to be more sector-specific (e.g., financial institutions, medical institutions and location-based service providers), this chapter will focus on the regulatory framework, new developments and issues related to the PIPA and the Network Act.

II THE YEAR IN REVIEW

i Legislative and regulatory changes

In April 2017, the National Assembly passed an amendment to the PIPA that requires data handlers to clearly indicate important information in a legally prescribed manner that is easily noticeable by data subjects when obtaining consent for the collection, use and provision of personal information. This amendment was passed after a recent decision by the Supreme Court of Korea invalidated consent for the collection of personal information because the size of the letters in the consent form used to obtain the consent was considered to be too small for data subjects to clearly notice and understand the contents therein. The Supreme Court’s decision overturned previous decisions by the trial court and appellate court affirming the validity of consent obtained through the same consent form. Consequently, this latest amendment to the PIPA appears to be a legislative solution to resolve any lingering controversy over whether consent obtained through a consent form that is difficult for data subjects to understand can be regarded as valid consent. This amendment is scheduled to take effect in October 2017 and specific matters on how to clearly present information and what type of information should be presented are expected to be set forth in the Enforcement Decree of the PIPA.

Apart from the foregoing amendment to the PIPA, there have not been many legislative developments regarding data protection laws in Korea, but several proposed amendments to the PIPA and the Network Act are currently under review in the National Assembly.
Notably, certain proposed amendments seek to introduce the de-identification methods set forth in the Guidelines for the PIPA and the Network Act, respectively, to expand the types of personal information that can be used by data handlers and online service providers.

In March 2017, the Enforcement Decree of the Network Act was amended to supplement the March 2016 amendment of the Network Act, which obligated online service providers (e.g., smartphone app developers) wishing to access stored data or functions within a user’s smartphone to disclose certain information (e.g., the stored data or function accessed and reasons for access) to users prior to obtaining their consent to the granting of access. Under the amended Enforcement Decree of the Network Act, the user’s prior consent will be required to access data within a user’s mobile device (e.g., smartphones and tablets) that (1) the user has stored by himself or herself (e.g., contact information, photos or bio data), (2) has been generated and stored automatically (e.g., location data, communication records or physical activity records), (3) constitutes particular identification information that can be easily traced to a specific individual, such as an International Mobile Equipment Identity, or (4) relates to input or output functions of the mobile device (e.g., photo and video recording, voice recognition or sensors). Additionally, the amended Enforcement Decree of the Network Act requires online service providers to distinguish between access that is inevitably necessary to provide the subject services and access that is not. This distinction should be made after considering factors such as (1) the scope of the subject services disclosed in the terms of use or privacy policy, (2) the actual services that are provided, (3) whether the services are reasonably foreseeable to users, and (4) the technical relationship between the subject services and the requested access authority.

The PIPA requires data handlers to implement certain physical, managerial and technical safety measures set forth in the Standards of Personal Data Security Measures (the Standards), an implementing regulation of the PIPA issued by the Ministry of Interior and Safety (MOIS) to ensure the secure processing of personal information. On 31 August 2017, the MOIS announced an amendment to the Standards that classifies data handlers into three tiers based on business scale and the amount of personal information in their possession, and that prescribes progressively stricter safety measures accordingly.

The PIPA provides that the MOIS is entitled to facilitate the self-regulation of data handlers for the protection of personal information. In this regard, if an association comprised of companies within a specific industry meets certain requirements, the MOIS will designate the association as a self-regulatory industry group so that it may establish data protection standards suited to its specific industry and require member companies to comply with those standards. Data handlers that are compliant with standards established by a duly designated self-regulatory industry group will be afforded certain benefits, such as being exempted from periodic investigations conducted by the MOIS. As of 2016, a total of seven associations (e.g., the Korean Hospital Association, the Korea Association of Realtors and the Korea Association of Travel Agents) were designated as self-regulatory industry groups and, in 2017, the Korean Medical Association, the Association of Korean Medicine, the Korean Dental Association and the Korean Pharmaceutical Association became newly designated.

ii Major data breaches

In March 2017, the computer network of a hotel reservation application was hacked resulting in the leaking of 3.4 million items of personal information and nearly 1 million items of booking information. The hackers leaked the information online and through emails and SMS after the application company refused their demands for payment. Although all of the hackers
were subsequently apprehended by law enforcement authorities and no monetary damage was reported among users of the hotel reservation application, this leak raised considerable invasion-of-privacy concerns because of the sensitive nature of the leaked information.

In June 2017, a major virtual currency exchange in Korea was hacked resulting in the leaking of the personal information of at least 30,000 users and certain users suffered monetary damage after losing their virtual currency through subsequent ‘voice phishing’ scams that may have been initiated by using the personal information obtained from the virtual currency exchange. The full scale of the leakage is expected to be disclosed by law enforcement authorities during the course of the ongoing investigation and the victims who suffered monetary damage are expected to initiate a lawsuit against the virtual currency exchange to demand compensation.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The framework act for the protection of personal data is the PIPA, which regulates processing of personal information by governmental and private entities. More exactly, all governmental agencies, legal entities, organisations and persons that process personal information in organised methods (the data handler, similar to the concept of the ‘controller’ under EU Directive No. 95/46/EC (General Data Protection Regulation)) are subject to the PIPA. Under the PIPA, personal data is categorised into personal information, sensitive information and unique identification information, and each type of information is defined as follows:

a Personal information is defined as information that pertains to a living individual and by which the individual can be identified (e.g., name or resident registration number). Even when an individual cannot be identified by certain information on its own, the information shall be regarded as personal information if the individual can be identified by easily combining the information with any other information.

b Sensitive information is defined as personal information regarding an individual’s ideology, faith, trade union or political party membership, political views, health, sexual orientation and other personal information that may cause a material breach of privacy (genetic information and criminal records are listed as other sensitive information in the Presidential Decree of the PIPA).

c Unique identification information is defined as identification information assigned to each individual by relevant laws such as resident registration numbers (RRNs), passport numbers, driver licence numbers and foreigner registration numbers.

To process sensitive information or unique identification information, the data handler must obtain the data subject’s express consent separate from the consent to the processing of other personal information. With respect to RRNs, data handlers may not collect and use RRNs, unless an exception applies under the PIPA or any other law.

The processing of personal information by online service providers, including telecommunication service providers, is regulated by the Network Act. The Network Act will, in principle, prevail over the provisions of the PIPA for the processing of personal information by online service providers, and the PIPA will be applied to matters that are not covered in the Network Act. The meaning of personal information under the Network Act is identical to the meaning under the PIPA, except that the personal information under the Network Act is limited to the personal information of the user who is using the service provided by
the online service provider. Unlike the PIPA, the Network Act does not provide definitions of sensitive information and unique identification information. However, the Network Act distinguishes essential personal information (personal information that is necessary for the provision of online services) and optional personal information (personal information that is not necessary for the provision of such services). Online service providers may refuse to provide their services to users who do not consent to the collection and use of essential personal information, but they may not refuse their services to users on the grounds that the user did not consent to the collection and use of optional personal information. Consequently, in practice, service providers are required to obtain consent for the processing of essential personal information and consent for the processing of other personal information separately to ensure that users’ consent to the processing of other personal information remains optional. Thus, online service providers will be required to obtain users’ separate consent to process any of their sensitive information or unique identification information because this information will not be essential personal information in most cases. The processing of RRNs is allowed only when such processing is allowed by the Network Act or other laws.

The basic regulatory schemes for the protection of personal information under the PIPA and the Network Act are substantially similar to each other, and these regulatory schemes include:

a. notice and consent requirements for the processing of personal information;

b. technical and managerial protection measures that are required to be taken by data handlers;

c. other obligations of data handlers, such as disclosure of privacy policies and appointment of privacy officers;

d. the rights of data subjects; and

e. data handlers’ obligations in relation to data leakage, such as reporting obligations to government agencies and payment of damages to data subjects.

The regulatory scheme for the protection of personal credit information under the Credit Information Act is also similar to those under the PIPA and the Network Act, but the details are quite different because of sector-specific characteristics.

### General obligations for data handlers

To ensure the right of data subjects to control their personal information, data handlers are required to obtain express opt-in consent from data subjects prior to processing the data subjects’ personal information.

Under the PIPA, data handlers are required to obtain this consent by notifying data subjects of:

a. the purpose of collection and usage;

b. the items of personal information that will be collected;

c. the retention and usage period of the collected personal information; and

d. the fact that data subjects are entitled to withhold consent, and of any disadvantage that would follow such a rejection.

If a data handler seeks to transfer personal information to a third party for the benefit of that third party, data handlers are required to obtain separate consent from the data subject after disclosing:

a. the name of the third party;
the third party’s purpose for using the personal information;
the items of personal information to be provided to the third party;
the retention and usage period enjoyed by the third party; and
the fact that the data subject can withhold consent, and any disadvantage that would follow such a rejection.

If personal information is outsourced to a third party for the benefit of the data handler, the data handler is required to disclose certain items about the outsourcing agreement (i.e., the name of the outsourced data processor and outsourced tasks) usually through its privacy policies; and enter into a written outsourcing agreement or some type of other similar document. For the processing of sensitive information and particular identification information, separate notice and consent are required.

The notice and consent requirements under the Network Act are very similar to the requirements under the PIPA. However, one difference between the PIPA and the Network Act is that the Network Act requires online service providers to obtain users’ consent before outsourcing the processing of personal information to a third party unless the outsourcing is necessary for the provision of their services and enhances the convenience of the user. If the outsourcing is necessary for the provision of their services and enhances the convenience of the user, the user’s personal information can be transferred without the consent of the user and only with disclosure of certain items through its privacy policy.

There are slight differences in the rights of data subjects and users under the PIPA and the Network Act, respectively. However, the basic rights of data subjects and users can be categorised as:

- the right to request suspension of processing of his or her personal information, or the right to withdraw his or her consent to the processing of personal information;
- the right to review processed personal information;
- the right to request correction of false personal information; and
- the right to obtain relief for damage caused by violation of the PIPA or the Network Act.

### iii Specific regulatory areas

Children’s personal information is also protected by the PIPA and the Network Act. If data handlers and online service providers seek to process the personal information of children under the age of 14, they are required to obtain the consent of the children’s legal guardians, and the legal guardians are authorised to exercise the children’s rights under the PIPA and the Network Act.

In addition to the PIPA, the Network Act and the Credit Information Act, there are many other laws that regulate the processing of specific types of personal information. For example, the processing of (personal) location information by location-based service providers will be subject to the Location Information Act, the medical information of patients is protected by the Medical Service Act and the Pharmaceutical Affairs Act, and

---

2 Such an agreement or document must include certain provisions such as:

- the purpose and scope of the outsourcing agreement;
- a prohibition on the processing of personal data that exceeds the scope of the outsourcing agreement;
- matters related to technical and managerial protection of personal information;
- a prohibition on subcontracting by the outsourced data processor; and
- the outsourced data processor’s liabilities for any breach of its obligations.
the secrecy of communications is protected by the Act on Protection of Communication Secrecy. The Elementary and Middle School Education Act prescribes matters related to the protection of educational records. The Act on Real Name Financial Transactions and Confidentiality requires employees and officers of financial institutions to keep financial transaction information confidential and prohibits the disclosure of such information.

iv Technological innovation and privacy law

There has been a lot of discussion about countermeasures against new threats to the protection of personal information because of new technical innovation, and the need to balance protection and commercial use of personal information; some of this discussion has resulted in regulatory or legislative changes.

For example, the Act on Development of Cloud Computing and Protection of Users (Cloud Computing Act) was enacted in March 2015 and subsequently became effective in September 2015. Although most provisions of the Cloud Computing Act are about the promotion and development of the cloud computing industry, several requirements for the protection of users’ information were introduced by the Act, such as:

a the obligation to notify users and government agencies in the event of data leakage;

b the right of users to request information on the country where the server for storing the users’ information is located;

c a prohibition on the disclosure or use of users’ information; and

d notice and consent requirements for providing users’ information to a third party.

To relieve location-based service providers from excessive regulation, the Act on Protection and Usage of Location Information (Location Information Act) was amended and became effective in August 2015. Under the amended Location Information Act, a location service provider that uses non-personal location information is not required to obtain a licence from the Korea Communications Commission (KCC) for the operation of a location-based service. In addition, location service providers can now provide data subjects with periodic notice on the provision of the data subject’s location information to a third party designated by the data subject if it previously obtained the user’s consent (prior to the amendment, location service providers were required to provide notice every time they provided location information to a third party designated by the data subject).

In August 2015, the Financial Supervisory Service (FSS) announced its policy to prevent financial fraud, such as voice phishing. Based on the assumption that fraudsters usually withdraw their victims’ money through ATMs, the FSS will induce banks to introduce new facial-recognition technology that will prevent financial transactions at ATMs if the user is concealing his or her face with sunglasses, a hat, etc.

The March 2016 amendment of the Network Act (providing a new consent requirement for online service providers (e.g., smartphone app developers) wishing to access stored data or functions within a user’s smartphone) appears to have been made in response to the increased use of smartphones and tablet PCs.

In addition, the KCC announced the Guidelines for the Protection of Personal Information in Online Targeted Advertisements (the Online Targeted Advertisement Guidelines) in February 2017 for the purpose of ensuring the transparency of online tracking

3 The Ministry of Science and ICT can recommend that cloud service providers or online service providers disclose this country information if it is necessary for the protection of users.
measures and the rights of users to control their exposure to behavioural advertisements. Specifically, a business operator that seeks to place an online behavioural advertisement or collects the information of users through online tracking in connection therewith must (1) provide notice of certain information regarding the collection of behavioural information and the options available to the user to control the collection in a manner that can be easily understood by the user; and (2) provide users with methods to decide for themselves whether to provide their behavioural information and receive online targeted advertisements through advertisements or through user devices (e.g., web browsers and smartphones).

Despite regulatory and legislative changes, and previous regulation of the introduction of new technology, most data protection issues arising from technological innovations are subject to the regulations under the current PIPA, the Network Act and other privacy-related laws.

IV INTERNATIONAL DATA TRANSFER

In June 2017, Korea joined the APEC Cross-Border Privacy Rules (CBPR), and the Korea Internet and Security Agency (KISA) is preparing an application for recognition as an Accountability Agent under the CBPR. On the other hand, Korea has yet to obtain recognition as a non-EU country providing adequate data protection under EU Directive No. 95/46/EC, although the European Commission is known to be assessing the adequacy of Korean data protection regulations currently.

Under the PIPA, if a data handler transfers personal information to a foreign entity for the benefit and use of that entity, the notice and consent requirements discussed in Section III.ii apply. In addition, the agreement for the transfer must be in compliance with the PIPA. However, if the processing of personal information is outsourced to a foreign entity, the notice and consent are not required, but the requirements for outsourcing (i.e., disclosure and outsourcing documents) explained in Section III.ii apply.

Originally, the Network Act did not make these distinctions between transfer and outsourcing. After the March 2016 amendments to the Network Act became effective, online service providers were permitted to transfer the personal information of users abroad without obtaining user consent under certain conditions (i.e., if the personal information is transferred (for the benefit of the online service provider) for the purposes of outsourcing its processing or storage to a third party; the outsourcing or storage is necessary for the provision of the online service provider's services and enhances the convenience of the user; and the online service provider has disclosed all required matters via its privacy policy or individually notified users via a statutorily prescribed method such as email).

V COMPANY POLICIES AND PRACTICES

Under the PIPA and the Network Act, data handlers and online service providers are required to implement measures necessary for the secure processing of personal information. These

---

4 Online service providers have been required to disclose the installation of applications (e.g., cookies) that automatically collect personal information, such as internet access logs, and the method for denying such installations in their privacy policy pursuant to the Network Act. In addition, data handlers and online service providers have been required to encrypt certain information during transmission or storage by the PIPA and the Network Act.
measures include technical and managerial protection measures, disclosure of the privacy policy, appointment of a (chief) privacy officer and supervision of outsourced data processors (if applicable). In addition, the PIPA requires the operator of CCTV or network cameras to establish a management plan for operation, and the Network Act requires online service providers to obtain prior opt-in consent from users to transmit advertising information to them through electronic means. The Network Act also requires certain online service providers to appoint a chief information security officer, to obtain certification of their security measures and to provide users with a periodic summary of any personal information that was processed.

i Protection measures
Data handlers and online service providers are required to implement technical and managerial protection measures, such as:

a. the establishment of an internal management plan for secure processing of personal information;
b. the implementation of a system or measures to prevent unauthorised access to personal information;
c. the use of encryption technology for secure transmission and storage of personal information;
d. the implementation of measures for secure storage of log data used to access personal information and the prevention of any forgery or falsification of the log data;
e. the installation of security programs (e.g., firewalls and anti-virus programs); and
f. the implementation of any other measures necessary for the secure processing of personal information.

The Standards issued by the MOIS stipulate the details of these protection measures. On 31 August 2017, the MOIS announced an amendment to the Standards that classifies data handlers into three tiers based on business scale and the amount of personal information in their possession and that prescribes progressively stricter safety measures accordingly.

ii Privacy policy
Data handlers and online service providers are required to disclose their privacy policies, usually through their website. The privacy policy shall include information on:

a. the items of personal information to be processed;
b. the purpose of processing the personal information;
c. matters concerning the transfer or outsourcing of personal information to third parties;
d. the period of retention and use of personal information;
e. matters related to the destruction of stored personal information; and
f. the rights of data subjects or users and the process of exercising those rights.

The privacy policy under the PIPA must also include information regarding protection measures. The privacy policy under the Network Act must include information on the installation of applications (e.g., cookies) that automatically collect personal information such as internet access logs, and the methods on how to avoid such an installation, and the name and contact information of the (chief) privacy officer or department in charge of personal information protection.
iii Chief privacy officer

Under the PIPA, all data handlers are required to appoint a person who is responsible for the processing of personal information (the chief privacy officer or personal information protection manager). The chief privacy officer or personal information protection manager is responsible for the following tasks:

- establishment and implementation of an internal policy for the protection of personal information and a privacy policy;
- regular inspection of the standards and procedures for processing personal information;
- addressing and resolving complaints related to the processing of personal information;
- establishment of an internal management system for the prevention of leakage and misuse of personal information;
- establishment and implementation of an internal plan for education on the protection of personal information;
- protection and management of personal information, including management of data related to personal information protection; and
- deletion of personal information.

Under the Network Act, online service providers are also required to appoint a chief privacy officer subject to certain exemptions (e.g., an online shopping service provider with fewer than five full-time employees).

iv Supervision of outsourced data processors

As explained above, when outsourcing the processing of personal information, data handlers are required to disclose certain items about the outsourcing agreement (i.e., the name of the outsourced data processor and outsourced tasks), usually through their privacy policies; and enter into a written outsourcing agreement or some other similar type of document. In addition, the data handler is required to supervise the outsourced data processor to prevent leakage, forgery, falsification and other damage to personal information. If any damage is caused to the data subject by the outsourced data processor’s violation of the PIPA in the course of processing personal data, the data handler will be subject to vicarious liability for any related compensation claim. Online service providers are subject to similar disclosure and supervision obligations and liability (i.e., vicarious liability for any compensation claim against an outsourced data processor for violations in the course of processing personal data).

VI DISCOVERY AND DISCLOSURE

i Disclosure to a national government

The process required for the disclosure of personal information in response to requests by a national government, investigation agency or court orders depends on the entity that is being requested to disclose the personal information. Under the PIPA, government agencies and certain public entities are widely exempted from ‘notice and consent’ requirements for the provision of personal information to third parties. For example, government agencies and certain public entities can provide personal information without the data subject’s consent if it is necessary for:

- the provision of personal information to a foreign government or international organisation to implement a treaty or some other international administrative agreement;
- a criminal investigation or regulatory inquiry;
c performance of a judicial function by the courts; or
d execution of a criminal sanction.

In contrast, the exceptions for private entities are very limited. Private entities can provide personal information without the data subject’s consent only when such a provision is required by other laws (e.g., a court warrant in a criminal investigation or other legal administrative investigation, or a duly authorised government order). A document production order by the court may compel a private entity to provide personal information to the court without the data subject’s consent. However, the Civil Procedure Act in Korea does not have extensive discovery procedures like the discovery process in the United States, so document production orders are likely to be approved in only limited circumstances.

ii Disclosure to foreign governments
Despite some controversy over whether foreign investigation agencies or courts can be provided with personal information by Korean government agencies or private entities in accordance with the exceptions in the PIPA (i.e., without the consent of the data subjects), the negative view (i.e., that foreign investigation agencies or foreign courts cannot be provided with personal information without the Korean data subjects’ consent) is more widely accepted. Even in view of this trend, if Korean government agencies or certain public organisations were to provide personal information without the data subjects’ consent, they would probably still be in compliance with the PIPA if such provision was necessary for the implementation of a treaty or some other international administrative agreement. However, if a Korean governmental entity provided personal information for some other purpose (not falling under the exceptions above), or if a Korean private entity provided personal information to a foreign government, there is a high possibility that the provision of personal information would be in violation of the PIPA if there was no prior consent given by the data subject.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies
The MOIS is responsible for the enforcement of the PIPA. To check whether data handlers are in violation of the PIPA, the MOIS can request data handlers to submit relevant documents and other materials, and can perform on-site investigations. If any violation is found, the MOIS can issue corrective orders or impose administrative fines on the data handlers. The MOIS can also refer the case to a criminal investigation agency. The Personal Information Protection Commission, which was established in accordance with the PIPA, is responsible for:

a the deliberation and resolution of government policy for the protection of personal information;
b the improvement of systems related to the protection of personal information and recommendations to government agencies;
c the survey of compliance levels of data handlers; and
d research for the improvement of laws and systems for the protection of personal information.
The regulatory authorities responsible for the enforcement of the Network Act are the KCC and the Ministry of Science and ICT (MSIT). The KCC is mainly responsible for matters related to the protection of personal information, and the MSIT is mainly responsible for matters related to cybersecurity. The KCC and the MSIT both possess investigatory and sanctioning authority similar to that of the MOIS. Some working-level tasks of the MOIS, the KCC and the MSIT are delegated to the KISA and the National Information Society Agency.

Recently, the Korea Fair Trade Commission (KFTC) has been expanding its involvement into the regulation of the protection of personal information. The KFTC regards the privacy policy and consent language for the processing of personal information as a standardised contract, and makes recommendations where amendments to these are deemed to be unfair to data subjects or users in violation of the Act on the Regulation of Standardised Contracts. For example, the KFTC issued a corrective order and imposed an administrative fine on a hypermarket chain reasoning that raffle ticket events used for the collection of personal information constituted fraudulent advertising and the consent language used for the processing of personal information constituted a standardised contract.

ii Recent enforcement cases
For recent enforcement cases, see Section II.

iii Private litigation
Under the PIPA, a class action is allowed in very limited situations. A class action raised against a data handler to require it to cease and desist from its purportedly unlawful activity can only be initiated by certain consumer organisations or non-commercial private organisations if the data handler has refused to comply with the decision of, or participate in a hearing supervised by, the Personal Information Dispute Mediation Committee organised under the PIPA. Because of these limitations on class actions, no class action suits have been initiated to date in Korea.

There have been numerous civil actions brought by data subjects and users seeking compensation for damage caused by leakage of their personal information handled by data handlers and online service providers. As large amounts of personal information have been leaked in data breach incidents, a great number of plaintiffs have collectively brought lawsuits against data handlers and online service providers. Most of the claimants in these lawsuits have sought compensation for mental distress caused by personal information leakage because it remains difficult to prove the actual monetary damage caused by the leakage. The most effective arguments in defence of data handlers and online service providers have been to emphasise that there were no violations of the PIPA or the Network Act because the defendants complied with the Standards and other similar standards under the PIPA.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Neither the PIPA nor the Network Act contains a specific provision addressing the issue of jurisdiction. If a subsidiary or branch office of a global organisation in Korea provides personal information to its headquarters outside Korea, this provision will trigger the issues related to international data transfer explained in Section IV.

For foreign organisations that directly process Koreans’ personal information, the relevant Korean regulators, especially the KCC, take the position that if the foreign organisation is targeting Korean users, the organisation is subject to Korean privacy laws and
regulation. In deciding whether the foreign organisation is targeting Korean users, the KCC will mainly consider whether the organisation has a website in the Korean language, whether the organisation is performing promotional activities to Koreans and whether the systems for the processing of personal information are located in Korea.

There have been a few cases where jurisdiction became an issue. In a case involving a violation of the Network Act by a foreign online service provider, the KCC took the position that a foreign online service provider that operates its server in a foreign country but operates its website in the Korean language and engages in the promotion of its online advertising business is subject to the requirements under the Network Act.

IX CYBERSECURITY AND DATA BREACHES

As previously explained in Section V.i, data handlers and online service providers are required to implement technical and managerial protection measures. The details of the measures for data handlers are prescribed in the Standards. The detailed measures for online service providers are prescribed in the regulation established by the KCC in accordance with the Network Act.

In the event of personal information leakage, the data handler is required to notify the affected data subjects immediately after the data handler becomes aware of the leakage. The notification to the data subject by the data handler shall include:

- the items of leaked personal information;
- the time and circumstances of the leakage;
- measures that can be taken by the data subject to prevent damage;
- the data handler’s countermeasures in response to the leakage and the process for remedying any damage; and
- the department responsible for receiving the data subject’s complaint and the relevant contact information.

If the volume of leaked personal information exceeds a certain level, the data handlers are required to report the incident directly to the MOIS or some other designated government agency.

The notification and report requirements for data leakage under the Network Act are very similar to the requirements under the PIPA. However, in the absence of a justifiable reason, the notification and report under the Network Act must be made within 24 hours of the moment the online service provider becomes aware of the leakage, and all personal information leakage incidents must be reported to the KCC or the KISA. Under the Network Act, if an online service provider becomes aware of an unauthorised intrusion into its network or information system caused by hacking, a computer virus, logic bomb, email bomb, denial of service or high-powered electromagnetic wave, the online service provider is required to report the incident to the MSIT or KISA. The MSIT may request the online service provider to submit materials related to the intrusion incident or it may conduct an investigation on the premises of the online service provider.
X  OUTLOOK

With the continuing advance of the IT industry, and as foreign online services become more widespread, there has been increased discussion on the need to achieve the appropriate balance between the right to control personal information and the commercial use of personal information. Such discussions will hopefully lead to more practical legislative or regulatory changes in the near future.

Most of the recent amendments to the PIPA, the Network Act and the Credit Information Act have yet to be applied to an actual case. Furthermore, the amendments to the Standards and the announcement of the Guidelines and the Online Targeted Advertisement Guidelines may have a considerable impact on ongoing efforts to achieve an optimal balance between the protection of personal data and the use of personal data. It will be interesting to follow the implications of these recent developments and their effect on future cases.
I OVERVIEW

The Personal Data Protection Act 2010 (PDPA), which came into force on 15 November 2013, sets out a comprehensive cross-sectoral framework for the protection of personal data in relation to commercial transactions.

The PDPA was seen as a key enabler to strengthen consumer confidence in electronic commerce and business transactions given the rising number of cases of credit card fraud, identity theft and selling of personal data without customer consent. Before the PDPA, data protection obligations were spread out among certain sectoral secrecy and confidentiality obligations, while personal information was primarily protected as confidential information through contractual obligations or civil actions for breach of confidence.

The PDPA imposes strict requirements on any person who collects or processes personal data (data users) and grants individual rights to ‘data subjects’. Enforced by the Commissioner of the Department of Personal Data Protection (the Commissioner), it is based on a set of data protection principles akin to the European Union (EU) principles and, for this reason, the PDPA is often described as European-style privacy law. An important limitation to the PDPA is that it does not apply to the federal and state governments.

The processing of information by a credit reporting agency is also exempted from the PDPA. In the past, credit reporting agencies did not fall under the purview of any regulatory authority in Malaysia, drawing heavy criticism for inaccurate credit information reporting. The Credit Reporting Agencies Act 2010, which came into force on 15 January 2014, now provides for the registration of persons carrying on credit reporting businesses under the regulatory oversight of the Registrar Office of Credit Reporting Agencies, a division under the Ministry of Finance, which is charged with developing a regulated and structured credit information sharing industry.

1 Shanthi Kandiah is a partner at SK Chambers. She was assisted in writing this chapter by Aida Harun and Carmen Koay, associates at SK Chambers.

2 EU Data Protection Directive 95/46/EC.

3 There is some ambiguity about which public entities fall within this definition. It does not appear that agencies and statutory bodies established under acts of parliament or state enactments to perform specific public functions, such as Bank Negara Malaysia (BNM), the Employees Provident Fund, the Securities Commission Malaysia and the Companies Commission of Malaysia, fall within the scope of this exemption.
i Cybersecurity
The PDPA enumerates the security principle as one of its data protection principles. Under this principle, an organisation must ensure both technical and organisational security measures are well in place to safeguard the personally identifiable information that it processes. The ISO/IEC 27001 Information Security Management System (ISMS), an international standard, which deals with information technology systems risks such as hacker attacks, viruses, malware and data theft, is the leading standard for cyber risk management in Malaysia.

Sectoral regulators such as BNM and the Securities Commission Malaysia have also been actively tackling issues relating to cybersecurity in relation to their relevant sectors by issuing guidelines and setting standards for compliance (discussed in Section IX).

The intersection between privacy and cybersecurity also manifests in the extent of the tolerance for government surveillance activity: the PDPA does not constrain government access to personal data, as discussed in Section VI. The reasons given to justify broad government access and use include national security, law enforcement and the combating of terrorism.

II THE YEAR IN REVIEW
The Commissioner has issued a Public Consultation Paper 4 entitled Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017 (the Proposed Order 2017), marking an important milestone in the personal data export restriction found in Section 129(1) of the PDPA. The Proposed Order 2017 seeks feedback from the public on the Commissioner’s draft whitelist of countries to which personal data originating in Malaysia may be freely transferred without having to rely on exemptions provided by Section 129(3) of the PDPA.5

The Commissioner has also moved towards the enforcement phase of PDPA implementation. In early May 2017, a company in the education industry was charged under the PDPA for processing the personal data of former employees without a certificate of registration.6

Several organisations in the following sectors have also received inspection visits from the Commissioner’s office: utility, insurance, healthcare, banking, education, direct selling, tourism and hospitality, real estate and services (retail and wholesale). Section 101 of the PDPA gives the Commissioner power to inspect the personal data systems in corporations with a view to making recommendations on compliance. The organisation is given limited notice of the pending visit. If an organisation fails to make the necessary improvements post inspection, this could lead to criminal enforcement action under the PDPA. An inspection visit from the Commissioner’s staff will entail a detailed review of the following areas:

a personal data collection forms and privacy notice;
b internal standard operating procedures for personal data management within the organisation;

5 See Section IX.
6 See Section VII.ii.
person in charge of personal data management within the organisation and his or her awareness of the legal requirements; and

d compliance with the seven data protection principles in the PDPA.

Complaints remain the primary trigger for the investigation and enforcement activities of the Commissioner. As of April 2017, the Commissioner has received over 330 official complaints since the coming into force of the law. Unsurprisingly, approximately 85 per cent of complaints relate to processing of data in the electronic environment.\(^7\)

Cybersecurity issues have also received significant media attention as Malaysian companies were not spared in the global ransomware attacks, such as the WannaCry cyberattack. On 9 June 2017, the deputy prime minister of Malaysia, Datuk Seri Dr Ahmad Zahid Hamidi, announced that the Malaysian government will introduce a new law that is aimed at protecting Malaysians from cybersecurity threats in light of the fact that there are about 10,000 cybersecurity-related reports received every year by the government. Malaysia does not have a specific law addressing cybersecurity-related offences. Enforcement agencies, such as the National Cyber Security Agency (NCSA), have to rely on existing legislation, such as the Communications and Multimedia Act 1998 (CMA), the Defamation Act 1957 and the Sedition Act 1948, to combat cyberthreats. It is expected that the NCSA would be placed under the umbrella of the National Security Council\(^8\) and will function as the agency that coordinates all efforts to manage cyberthreats.

### III REGULATORY FRAMEWORK

#### i Privacy and data protection legislation and standards

The PDPA is a comprehensive data protection legislation containing seven data protection principles, including the general principle establishing the legal requirements for processing personal data (e.g., with consent or in compliance with the legal requirements), notice (internal privacy notices for employees and external notices for consumers), choice, disclosure, data security, integrity and retention, and rights of access. Failure by an organisation to observe these principles is an offence.\(^9\) The Personal Data Protection Standards 2015, which came into force on 23 December 2015 (the Standards) are considered the 'minimum' standards to be observed by companies in their handling of personal data of customers and employees, and failure to implement them carries criminal sanctions.

The PDPA also sets up a co-regulatory model that emphasises the development of enforceable industrial codes of practice for personal data protection against the backdrop of the legal requirements of the government. Codes of Practice that have been approved and registered by the Commissioner include the Personal Data Protection Code of Practice

---

7 Conference on the PDPA organised by the Personal Data Protection Department at Hotel Istana, Kuala Lumpur on 23 May 2017.

8 The National Security Council is a federal agency under the Prime Minister’s Department and is responsible for managing and coordinating the implementation of policies related to the security of Malaysia.

9 Section 5(2) of the PDPA.
for the Utilities Sector (Electricity), 10 the Personal Data Protection Code of Practice for the Insurance/Takaful Industry11 and the Personal Data Protection Code of Practice for the Banking and Financial Sector.12

Non-compliance with the codes will also carry penal consequences.13

**Personal data**

Three conditions must be fulfilled for any data to be considered as ‘personal data’ within the ambit of the PDPA.14

First, the data must be in respect of commercial transactions. ‘Commercial transactions’ is defined under the PDPA as transactions of a commercial nature, whether contractual or not, and includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.15 There is some ambiguity as to whether an activity must have a profit motivation to be considered a commercial transaction.

Second, the information must be processed or recorded electronically or recorded as part of a filing system.

Third, the information must relate directly or indirectly to a data subject who is identifiable from the information or other information in the possession of the data user. A central issue for the application of the PDPA is the extent to which information can be linked to a particular person. If data elements used to identify the individual are removed, the remaining data becomes non-personal information, and the PDPA will not apply.16

**Sensitive personal data**

Sensitive personal data is defined as any personal data consisting of information as to:

- the physical or mental health or condition of a data subject;
- his or her political opinions;
- his or her religious beliefs or other beliefs of a similar nature;
- the commission or alleged commission by him or her of any offence; or
- any other personal data as the minister responsible for personal data protection (currently the Minister of Communications and Multimedia) may determine.17

Sensitive personal data may only be processed with the explicit consent of the data subject and in the limited circumstances set out in the PDPA.18

**Application of the PDPA**

The PDPA applies to any person who processes or has control over the processing of any personal data in respect of commercial transactions.

10 With effect from 23 June 2016.
11 With effect from 23 December 2016.
12 With effect from 19 January 2017.
13 Section 29 of the PDPA.
14 Section 2 of the PDPA.
15 Section 2 of the PDPA.
16 See also Section 45(1)(c) of the PDPA.
17 Section 2 of the PDPA.
18 Section 40(1) of the PDPA.
'Processing' has been defined widely under the PDPA to cover activities that are normally carried out on personal data, including collecting, recording or storing personal data, or carrying out various operations such as organising, adapting, altering, retrieving, using, disclosing and disseminating the data.

Most of the obligations under the PDPA apply to a ‘data user’ (i.e., ‘a person who either alone or jointly in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor’).

A ‘data processor’ who processes personal data solely on behalf of a data user is not bound directly by the provisions of the PDPA.

### General obligations for data users

#### Registration

The Personal Data Protection (Class of Data Users) Order 2013 lists 11 categories of data users who have to be registered with the Commissioner. The categories are:

- a banking and finance;
- b insurance;
- c telecommunications;
- d utilities;
- e healthcare;
- f hospitality and tourism;
- g education;
- h real estate and property development;
- i direct selling;
- j services (e.g., legal, accountancy, business consultancy, engineering, architecture, employment agencies, transportation); and
- k retail and wholesale.

The list of data users has been expanded in 2016 to include two additional sectors: pawnbroking and money lending.\(^{19}\)

Failure to register by these categories of data users is an offence.\(^{20}\)

#### Purpose limitation

A data user may not process personal data unless it is for a lawful purpose directly related to the activity of the data user, the processing is necessary and directly related to the purpose, and the personal data are adequate and not excessive in relation to that purpose.

The data subject must also consent to the processing of the personal data unless the processing is necessary for specific exempted purposes.\(^{21}\)

#### Consent

The PDPA does not define ‘consent’; nor does it prescribe any formalities in terms of the consent. However, the Personal Data Protection Regulations 2013 (the Regulations) provide

---

19 Personal Data Protection (Class of Data Users) (Amendment) Order 2016, which came into effect on 16 December 2016.

20 Section 16(4) of the PDPA.

21 Section 6(2) of the PDPA.
that the data user must keep a record of consents from data subjects. The Regulations further provide that the Commissioner or an inspection officer may require production of the record of consents. It places the burden of proof for consent squarely on the data user.

Helpfully, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides examples of consent, whether express or implied, that must be recorded or maintained by the data user. These examples include:

a signatures, or a clickable box indicating consent;
b deemed consent;
c verbal consent; and
d consent by conduct or performance.

Consent is deemed given by way of conduct or performance if the data subject does not object to the processing; the data subject voluntarily discloses its personal data; or the data subject proceeds to use the services of the data user.

Verbal consent should be recorded digitally or via a written confirmation that consent was given.

Explicit consent

Regarding explicit consent, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides the following examples: where the data subject provides his or her identification card to be photocopied or scanned; where the data subject voluntarily provides the sensitive personal data; and verbal statements that have been recorded or maintained.

Notification

Data users are obliged to notify individuals of their purposes for the collection, use and disclosure of personal data on or before such collection, use or disclosure. For example, where a data user intends to use personal information collected for a different purpose, such as marketing communications, the data user must provide the affected individuals with the choice to disagree with the purpose before doing so.

Disclosure

Data users shall not disclose personal data for any purpose other than that for which the data was disclosed at the time of collection, or for a purpose directly related to it; or to any party other than a third party of the class notified by the data user without a data subject’s consent. 22

Retention

Personal data should not be kept longer than necessary. Retention policies must take into account any relevant requirements imposed by applicable legislation. However, the Standards appear to impose organisational requirements that may be challenging for organisations to comply with. Personal data collection forms are required to be destroyed within

---

22 If a data user is found guilty of disclosing personal data without the consent of the data subject, he or she may be liable to a 300,000-ringgit fine or two years’ imprisonment, or both.
a period of 14 days, unless the forms can be said to have some ‘legal value’ in connection with the commercial transaction. It is unlikely that this time frame would be feasible for most organisations.

A record of destruction should be properly kept and be made available when requested by the Commissioner.

Data subjects’ rights
A data subject has various rights to his or her personal data kept by data users. These are:

a the right of access to personal data; 23
b the right to correct personal data; 24
c the right to withdraw consent; 25
d the right to prevent processing likely to cause damage or distress; 26 and
e the right to prevent processing for purposes of direct marketing. 27

iii Technological innovation
In general, the regulatory framework has not developed specific rules (outside the application of the seven principles in the PDPA) to deal with data privacy issues created by cookies, online tracking, cloud computing, the internet of things or big data.

Government efforts appear to be focused on positioning the country appropriately to benefit from these innovations. For example, the Ministry of Science, Technology and Innovation has unveiled the National Internet of Things Strategic Roadmap (the Roadmap). Under the Roadmap, a centralised regulatory and certification body will be established to address privacy, security, quality and standardisation concerns.

iv Specific regulatory areas
There are special confidentiality rules that apply to data in specific sectors, such as the banking and financial institutions sectors, the healthcare sector as well as the telecommunications and multimedia sectors. However, these rules do not comprehensively cover all aspects of data protection in the comprehensive manner addressed by the PDPA, which tracks the information life cycle from its collection and use through to its storage, destruction or disclosure.

Minors
The PDPA does not contain specific protection for minors (below the age of 18). Section 4 of the PDPA states that for minors, the guardian or person who has parental responsibility for the minor shall be entitled to give consent on behalf of the minor.

23 Section 30 of the PDPA.
24 Section 34 of the PDPA.
25 Section 38 of the PDPA.
26 Section 42 of the PDPA.
27 Section 43 of the PDPA.
Financial institutions

A banker’s duty of secrecy in Malaysia is statutory as is clearly provided under Section 133(1) of the Financial Services Act 2013 (FSA). The duty is not absolute. Section 153 of the FSA provides the legal basis for BNM to share a document or information on financial institutions with an overseas supervisory authority.

The Guidelines on Data Management and MIS Framework issued by BNM sets out high-level guiding principles on sound data management and MIS practices that should be followed by financial institutions. It is noteworthy that boards of directors and senior management are specifically entrusted with the duty to put in place a corporate culture that reinforces the importance of data integrity.

Healthcare

The Medical Act 1971 is silent on the duty of confidentiality. The Confidentiality Guidelines issued by the Malaysian Medical Council in October 2011 after the PDPA was enacted are the most comprehensive articulation of the confidentiality obligation of health professionals.

Multimedia and telecommunications

The General Consumer Code of Practice (GCC), developed by the Communications and Multimedia Consumer Forum of Malaysia, sets out a number of consumer protection principles, one of which is the protection of consumers’ personal information (quite similar in scope to the seven PDPA principles) for the telecommunications and multimedia sectors. The GCC binds all licensed service providers under the CMA and all non-licensed service providers who are members of the Consumer Forum.

Direct selling

The PDPA prescribes direct sellers as one of the 11 classes of data users that must register with the Personal Data Protection Department.

The PDPA also gives consumers the right to request in writing that the direct seller stop or not begin processing their personal data. Failure to cease using personal data for direct marketing purposes after a data subject has objected could make the offender liable for a fine of up to 200,000 ringgit, imprisonment for up to two years, or both.

IV INTERNATIONAL DATA TRANSFER

Section 129(1) of the PDPA states that a company may only transfer personal data out of Malaysia if the country is specified by the Minister of Communication and Multimedia Malaysia and this is then published in the Gazette. The places identified in the Proposed Order 2017 are as follows: European Economic Area member countries, the United Kingdom, the

---

28 Schedule 11 of the FSA sets out a list of permitted disclosures.
29 See also Section 165 of the Islamic Financial Services Act 2013.
30 Management Information System.
31 The Malaysian Communications and Multimedia Content Code also sets out privacy related restrictions.
32 See Section II.
United States, Canada, Switzerland, New Zealand, Argentina, Uruguay, Andorra, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, Australia, Japan, Korea, China, Hong Kong, Taiwan, Singapore, the Philippines and Dubai International Financial Centre.

Until the Proposed Order 2017 comes into effect, to transfer data outside the country, organisations will have to rely on the exemptions set out in Section 129(3) PDPA, which include:

\[\begin{align*}
\text{a} & \quad \text{where the data subject has consented to the transfer;} \\
\text{b} & \quad \text{where the transfer is necessary for the performance of a contract between the data subject and the data user;} \\
\text{c} & \quad \text{where the transfer is necessary to protect the vital interests of the data subject; and} \\
\text{d} & \quad \text{where the data user has ‘taken all reasonable precautions and exercised all due diligence’ to ensure that the personal data will not be processed in the recipient country in a way that would be a contravention of the PDPA.}
\end{align*}\]

Unlike EU law, Malaysian law does not require transfer contracts to be made for the benefit of third parties. Malaysia also has a doctrine of privity of contract that prevents enforcement of third-party benefits by data subjects.

V COMPANY POLICIES AND PRACTICES

Organisations are under the obligation to implement policies and enforce certain practices to ensure their compliance with the PDPA.

i Data protection officers

The requirements for a data protection officer are not spelled out in specific terms as yet; however, these are likely to be specifically provided for in the near future. A Commissioner’s Proposal Paper (No. 2/2014), Guidelines on Compliance with Personal Data Protection 2010, makes a clear proposal for every organisation to establish responsibility for protection of personal data at the highest level and to designate an officer for this responsibility. The officer’s primary responsibility will be ensuring that all policies, procedures, systems and operations are aligned with the PDPA. There is, however, no requirement for a senior management position such as a chief privacy officer.

In addition, the proposed Guidelines appear to place the responsibility for protection of personal data at the highest level, which would appear to suggest that privacy should be a board level issue.

ii Online privacy policies

It is not uncommon for an organisation’s privacy policy to be used as a privacy notice. Privacy policies are sometimes used as a privacy notice in lieu of developing a separate document.

iii Internal privacy policies for employees’ rights and responsibilities

The notice and choice principle requires an employer to inform the employee of the nature of the information collected; whether the information will be shared with a third party; and that he or she has the right to access the information collected.
iv  
**Requirement for data privacy due diligence and oversight over third parties**

The Standards require data users, in discharging the security principle, to bind third parties contractually to ensure the safety of personal data from misuse, loss, modification, unauthorised access and disclosure. Some organisations do take the additional step of reserving audit rights over third parties processing personal data of their behalf, but this is not currently mandated.

v  
**Written information security plan**

The Regulations require that data users develop and implement a security policy for their companies. This security policy must comply with standards established by the Commissioner from time to time. Some of the more prescriptive standards for implementation are the standards stipulating that the transfer of personal data through removable media devices (e.g., USB thumb drives) and cloud computing services (e.g., Dropbox and Google Drive) is no longer permitted, unless authorised in writing by the ‘top management’ of the company.

Even when permitted, each transfer of personal data via such a removable media device must be recorded. Additionally, data users are required to record access to personal data, and to make the records available to the Commissioner upon request.

vi  
**Incident response plan**

Data breach management and incident response plans have not been mandated by the Commissioner.

VI  
**DISCOVERY AND DISCLOSURE**

The data protection provisions under the PDPA do not affect any rights and obligations under other laws. There is a clear exemption for disclosure of personal data for a purpose other than the purpose for which data was collected where the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations.

In this regard, Malaysian legislation (including the PDPA) tends to provide authorities with extensive powers of search and seizure, including powers to search without a warrant. This power arises where the delay in obtaining a search warrant is reasonably likely to adversely affect investigation, or where evidence runs the risk of being tampered with, removed or destroyed.

Section 263(2) of the CMA is particularly noteworthy. Internet service providers as licensees under the CMA must comply with the Malaysian Communications and Multimedia Commission or any other authorities that make a written request for their assistance in preventing an offence or the attempt of any crime listed under Malaysian law.

Section 263(2) is broad enough to permit authorities to gain access to telecommunications information such as contact information and content of communications.

33  
The Personal Data Protection Standards 2015.
VII  PUBLIC AND PRIVATE ENFORCEMENT

i  Enforcement agencies

The Commissioner has been entrusted with certain powers under the PDPA to enforce the PDPA. It has conferred powers to carry out inspections and investigations on data users, whether or not these are initiated by any complaints received from the public. The powers of the Commissioner include:

- conducting inspections on data users’ personal data systems;
- publishing reports that set out any recommendations arising from the inspections; and
- serving enforcement notices on data users for a breach of any of the provisions of the PDPA, and directing data users to take (or refrain from taking) specified steps to ensure that they comply with the PDPA.

The Commissioner’s authorised public officers also have various powers of enforcement under the PDPA, including:

- conducting investigations on the commission of any offence under the PDPA;
- conducting searches and seizure of data users’ computerised data, documents, equipment, systems and properties, with or without a warrant;
- requiring the production of computers, books, accounts, computerised data or other documents kept by data users; and
- arresting without warrant any person who the authorised public officer reasonably believes has committed or is attempting to commit an offence under the PDPA.

It is worth highlighting a provision that is now commonplace in Malaysian legislation (including the PDPA) that provides that where an offence is committed by a body corporate, its director, chief executive officer, chief operating officer, manager, secretary or other similar officer, the entity or person may be deemed to have committed the offence unless it, he or she can establish that there was no knowledge of the contravention, and that it, he or she has exercised all reasonable precautions and due diligence to prevent the commission of the offence.34

ii  Recent enforcement cases

In May 2017, a company operating a private college was charged with processing personal data without a certificate of registration under Section 16(4) of the PDPA. This offence carries a maximum fine of 500,000 ringgit or up to three years in jail, or both. This action is the very first case in Malaysia involving a breach of the PDPA. The office of the Commissioner has said that there are other cases in the pipeline.

iii  Private litigation

The PDPA does not provide for a statutory civil right of action for breach of any of the provisions of the PDPA. An aggrieved individual can nevertheless still pursue a civil action under common law or tort against a data user who has misused the individual’s personal data.

---

34  Section 133(1) of the PDPA.
VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to all activities relating to the collection, use and disclosure of personal data in Malaysia. As such, it will also apply to foreign entities processing such data in Malaysia regardless of whether they have an actual physical presence in Malaysia. The PDPA does not apply to personal data that is processed outside Malaysia, unless the data is intended to be further processed in Malaysia.

IX CYBERSECURITY AND DATA BREACHES

Statistics from Cybersecurity Malaysia for 2016 – MyCERT Incident Statistics – indicate that in 2016 alone there were over 8,000 reports on cyber-related incidents. This figure does not include those cases that go unreported almost daily, as there is no requirement to report breaches to the authorities or to customers.

The National Cyber Security Policy is Malaysia’s integrated cybersecurity implementation strategy to ensure the critical national information infrastructure (CNII) is protected to a level that is commensurate with the risks faced. Cutting across government machineries, the implementation has drawn in various ministries and agencies to work together to create a CNII that is secure, resilient and self-reliant. Implementation of this scheme has involved certification of CNII by Cybersecurity Malaysia to be ISMS-compliant.

BNM has also issued a circular on ‘Managing Cybersecurity Risks’, under which financial institutions are required to adhere to the ‘Minimum Measures To Mitigate Cyber Threats’. Measures include measures to:

- assess the implementation of multilayered security architecture;
- ensure security controls for server-to-server external network connections;
- ensure the effectiveness of the monitoring undertaken by Security Operation Centre to view security events, including incidents of all security devices and critical servers on a 24/7 basis; and
- subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and provide counter measures.

The Securities Commission Malaysia has also issued its Guidelines on Management of Cyber Risk, which sets out a framework to address cybersecurity resilience for capital market participants’ management of cybersecurity risks.

i Cyber laws

In contrast to the comprehensive approach of the PDPA, Malaysia’s cyber laws are scattered across various pieces of legislation, although this will be more streamlined when the proposed new cybersecurity law (which seeks to empower the NCSA to coordinate responses to cyberthreats) comes into effect. Presently, the key provisions of Malaysia’s cyber laws are as follows.

---

36 With effect from 31 October 2016.
CMA

Offences under the CMA include:

a. the offence of the use of network facilities or network services by a person to transmit any communication that is deemed to be offensive and that could cause annoyance to another person; 37

b. the offence of using an apparatus or device without authority; 38

c. the offence of improper use of network facilities or network services – such as annoying, abusive, threatening, harassing or obscene communications – emails (spamming), SMS or MMS website content publishing; 39

d. the offence of interception and disclosure of communications; 40 and

e. the offence of damage to network facilities. 41

Other cyber offences include:

a. cyber pornography and exploitation of children; 42

b. online sedition and internet defamation; 43

c. misuse of computers; 44

d. prostitution and other illegal cyber sexual activities; and

e. cyber terrorism. 45

ii  Laws to facilitate prosecutions of internet-based offences

A noteworthy development in Malaysian law was the introduction of Section 114A into the Evidence Act 1950, which came into force on 31 July 2012. Under the new Section 114, a person is deemed to be a publisher of a content if it originates from his or her website, registered networks or data-processing device of an internet user unless he or she proves the contrary.

iii  Laws to promote tracking transactions conducted on the internet

Examples of laws that provide for tracking and recording transactions conducted on the internet include the Cyber Centre and Cyber Cafe (Federal Territory of Kuala Lumpur) Rules 2012 and the Consumer Protection (Electronic Trade Transactions) Regulations 2012. The former require any person operating a cyber cafe and cyber centre to maintain a customer

37 Section 233(1)(a) of the CMA.
38 Section 231 of the CMA.
39 Section 233 of the CMA.
40 Section 234 of the CMA.
41 Section 235 of the CMA.
42 Sections 292, 293 and 294 of the Penal Code, Section 5 of the Film Censorship Act 2002 and Section 31 of the Child Act 2001.
43 Sections 3 and 4 of the Sedition Act 1948, Section 211 (prohibition on provision of offensive content) and Section 233 (improper use of network facilities or network service) of the CMA.
44 Section 3 (unauthorised access to computer materials), Section 4 (unauthorised access with intent to commit or facilitate commission of further offence), Section 5 (unauthorised modification of contents of any computer) and Section 6 (wrongful communications) of the Computer Crimes Act 1997.
45 The Penal Code contains provisions that deal with terrorism that may apply to cyber terrorism, such as Chapter VIA Sections 130B–130T (incorporated into the Penal Code on 6 March 2007).
entry record and a record of computer usage for each computer, whereas the latter require online business owners and operators to provide their full details and terms of conditions of sale, to rectify errors and maintain records.

X OUTLOOK

We expect to see more enforcement actions by the Commissioner in the coming year. In terms of inspection visits, the Commissioner’s focus appears to be set on sectors processing large quantities of personal data.

Compliance with the General Data Protection Directive (GDPR) is a topic we expect to see proactively addressed by Malaysian corporations that collect and process data of EU residents (such as customers, permanent residents, visitors and expatriates) given its extraterritorial reach and the looming implementation deadline of 25 May 2018. The GDPR’s prescriptions on organisational and technical measures to protect personal data are likely to influence Malaysian standard setting as well.

An area that would benefit from more explicit standard setting, given the ubiquitous reliance on the internet for commercial transactions, relates to the technological measures for protecting personal or sensitive personal data, such as data classification, data loss prevention, encryption, managing consent and data transfer limitations, as standards vary significantly in Malaysian corporations.

The installation of a centralised agency to enforce cybersecurity breaches in the country is a game changer. The precise jurisdictional scope and extent of powers given to this agency, however, remains unclear.
I OVERVIEW

The right to privacy or intimacy is contemplated in Paragraphs 1 and 12 of Article 16 of the Mexican Constitution, which prohibits anyone from intruding onto an individual’s person, family, domicile, documents or belongings (including any wiretapping of communication devices), except when ordered by a competent authority supported by the applicable law. The right to data protection is stipulated in Paragraph 2 of Article 16 of the Constitution, which seeks to set a standard for all collecting, using, storing, divulging or transferring (collectively processing) of personal data (as defined below) to secure the right to privacy and self-determination. The right to privacy and data protection are closely related fundamental rights that, along with other fundamental rights, seek to protect individuals’ ability to guard a portion of their lives from the intrusion of third parties. Notwithstanding this, while a breach of privacy usually results in a breach of the right to protection of personal data, a data protection breach does not always result in a breach of privacy.

The first formal effort to address personal data protection was introduced in 2002 when the Mexican Congress approved the Federal Law for Transparency and Access to Public Governmental Information (the Former Transparency Law). Although the Former Transparency Law was mainly aimed at securing access to any public information in the possession of the branches of government and any other federal governmental body, it also incorporated certain principles and standards for the protection of personal data being handled by those government agencies. This effort was followed by similar legislation at the state level.

After several attempts to address data protection rights more decisively, in 2009 Congress finally approved a crucial amendment to the Constitution that recognised the protection of personal data as a fundamental right. Consequently, Congress enacted the Federal Law for the Protection of Personal Data in Possession of Private Parties (the Private Data Protection Law), which became effective on 6 July 2010 and was followed by the Regulations of the Private Data Protection Law on 22 December 2011.

Additionally, in January 2014 Congress approved an amendment to the Constitution to create an autonomous entity to be in charge of enforcing the Private Data Protection Law and to take on the duties of the former Federal Institute for Access to Information and Protection of Data (the former IFAI), which was originally created as a semi-autonomous agency separate from the federal public administration. However, in a rather controversial move, the former IFAI amended its internal regulations so that it could assume the necessary

---

1 César G Cruz-Ayala is a partner and Diego Acosta-Chin is an associate at Santamarina y Steta, SC.
characteristics, and role, of the proposed autonomous entity. Consequently – and as a result of the new General Law for Transparency and Access to Public Governmental Information, which annulled the effect of the former Transparency Law – all matters previously dealt with by the former IFAI are now being handled by the ‘new IFAI’ as an autonomous entity; and it has adopted the title National Institute of Transparency, Access to Information and Protection of Personal Data (INAI).

The Private Data Protection Law is an omnibus data protection law that sets the principles and minimum standards that shall be followed by all private parties when processing any personal data. However, the Private Data Protection Law also recognises that standards for implementing data protection may vary depending on the industry or sector; accordingly, the Private Data Protection Law can certainly be complemented by sectoral laws and self-imposed regulatory schemes, which would focus on particular industry standards and requirements, to the extent that those standards and requirements comply with the data protection principles in the Private Data Protection Law. There have been efforts to promote such sector-specific rules among those processing any personal data within the same industry.

Finally, on 13 December 2016 the Mexican Congress approved the General Law for the Protection of Personal Data in Possession of Governmental Entities (the Governmental Data Protection Law, and collectively with the Private Data Protection Law, the Data Protection Laws), which was enacted on 27 January 2017, to establish a legal framework for the protection of personal data by any authority, entity or organ of the executive, legislative and judicial branches, political parties, and trust and public funds operating at federal, state and municipal level. On the understanding that this particular Law Review is intended to address issues arising from data protection in the private sector, we will not address in detail the Governmental Data Protection Law, unless it is necessary to add context.

The INAI is in charge of promoting the rights to protection of personal data, and enforcing and supervising compliance with the Data Protection Laws and those secondary provisions deriving from those Laws. To this end, with respect to the private sector, the INAI has been authorised to supervise and verify compliance with the Private Data Protection Law; interpret administrative aspects of the Data Protection Laws; and resolve claims and, inter alia, impose fines and penalties. The INAI has been actively working through media campaigns to raise awareness among corporations and individuals of the relevance of adequate protection of personal data. Although the INAI has the authority to initiate enforcement activities, most fines and penalties imposed have resulted from claims filed by data subjects. We are aware that companies that have been fined by the INAI for breaching the Private Data Protection Law have challenged the decisions by means of nullity claims and amparo lawsuits; however, the relevant files are not publicly available.

II THE YEAR IN REVIEW

During 2017, the INAI continued to enforce the Private Data Protection Law and has also redoubled its efforts to issue educational guidelines on proper processing of personal data for certain activities and also to increase awareness of the importance of protecting personal data.
III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The most relevant pieces of legislation addressing personal data protection in Mexico are the following:

a. the Constitution;
b. the Private Data Protection Law;
c. the Governmental Data Protection Law;
d. the Regulations of the Private Data Protection Law;
e. the Guidelines for Privacy Notices; and
f. the Self-Regulation Parameters on Data Protection, which are applicable to the private sector.

The Private Data Protection Law identifies those data protection principles governing all processing of personal data, as well as the obligations imposed on any private person, whether an individual or entity, that has control over the processing of personal data (a data controller), data processors (as defined below), third parties and any others engaged in the processing of personal data. As demanded by the Private Data Protection Law, the Mexican executive branch issued the Regulations of the Private Data Protection Law with the intention of clarifying the scope of those principles and obligations provided by the Private Data Protection Law. The Regulations also set out the rules applicable to the exercise by data subjects of their rights in relation to data controllers and those proceedings arising from claims before the INAI filed by data subjects in the event of a breach of the Private Data Protection Law by a data controller. Finally, the Guidelines for Privacy Notices (the Guidelines), issued by the Secretariat of the Economy, set the standard of detail that should be met by data controllers when drafting their own privacy notices and the scope of the language in privacy notices, and the Self-Regulation Parameters on Data Protection establish the rules, criteria and procedures for the development and implementation of self-regulatory schemes on data protection, and were also issued by the Secretariat of the Economy.

Both the Federal Consumer Protection Law and Federal Consumer Protection Law for the Users of Financial Services also contain stipulations protecting consumers, whether individuals or entities, from any processing of their information for marketing purposes. Corporations or financial entities that wish to market products must first review the list of consumers who do not wish to receive marketing information and recorded in the Public Registry of Consumers held by the Federal Consumers Attorney’s Office (Profeco), or the Public Registry of Individual Users, which is managed by the National Commission for the Protection of Financial Services Users (Condusef). Any marketing activity with any consumers enrolled in the registries may result in fines by Profeco or Condusef, as applicable.

Key definitions

In addition to any other terms defined herein, the following terms in particular should be taken into consideration for a better understanding of Mexican law on the subject:

a. data processor: any natural person or entity that individually or jointly with others carries out the processing of personal data on behalf of the data controller;
b. data subject: the natural person whom the personal data concerns;
personal data: any information related to an identified or identifiable individual. The following information would not be subject to the Private Data Protection Law:

- information collected and stored for personal use and not intended for divulgence or commercialisation;
- information collected by credit bureaux;
- information about entities;
- information about any individual when acting as a merchant or professional practitioner; or
- information about any individual when rendering services to a legal entity or to a merchant or professional practitioner, provided that information is limited to the subject’s name, duties or position, business address, business email, business telephone and business facsimile, and the information is processed when representing the merchant or professional practitioner;

d public access source: a database that may be accessed by anyone without complying with any requirement, except for the payment of a fee;

e sensitive personal data: personal data affecting the most intimate sphere of the data subject, or of which the misuse may be a cause for discrimination or great risk for the data subject, such as information regarding racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical or mental health, and sex life;

f transfer: any kind of communication of personal data made to a person other than the controller, data processor or data subject; and

g remittance: any kind of communication of personal data between the data controller and the data processor, within or outside Mexican territory.

Data protection principles

In consideration of the fact that the Private Data Protection Law is inspired by the European model provided in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on free movement of such data, the backbone of the Private Data Protection Law lies in the principles by which each data controller must abide to protect the personal data being processed by the same. These principles are summarised as follows:

a Legality: all personal data shall be lawfully collected and processed, and its collection shall not be made through fraudulent or deceitful means.

b Consent: all processing of personal data shall be subject to the consent (whether express or implied) of the data subject, with certain exemptions set out in the Private Data Protection Law. Nonetheless, when a data controller is processing any sensitive personal data, the data controller must obtain the express consent of the data subject to process this data, which must be evidenced in writing or through an electronic signature or any other authentication mechanism developed for that purpose. Exemptions to the requirement to obtain consent exist when:

- processing is permitted by law;
- the personal data are publicly available;
- processing prevents association between the personal data and the data subject or his or her identification because of the structure, content or grade of disaggregation of the personal data;
- processing is intended to comply with obligations resulting from a legal relationship between the data controller and the data subject;
• there is an emergency situation that may injure an individual or damage his or her assets;
• processing is essential for the purposes of rendering healthcare services or assistance, the application of preventive medicine, determination of medical diagnosis or the management of healthcare services, as long as the data subject is unable, in the terms provided by the General Health Law, to grant his or her consent for the applicable procedure; and
• a competent authority orders the processing.

c Quality: the data controller shall cause personal data in a database to be relevant, accurate and up to date for the purpose for which it is meant to be used, and shall only retain personal data for as long as is necessary to fulfil the specified purpose or purposes.

d Purpose: processing of personal data shall be limited to the purpose or purposes specified in the privacy notice. No database containing sensitive personal data shall be created without justifying that the purpose for its collection is legitimate, concrete and in compliance with those activities or explicit purposes sought by the data controller. Any processing of personal data for a purpose that is not compatible or analogous to what is set forth in the privacy notice shall require a new consent from the data subject.

e Proportionality: processing of personal data must be necessary, adequate and relevant for the purpose or purposes set forth in the privacy notice. With respect to sensitive personal data, reasonable efforts shall be made to keep the period of processing to a minimum.

f Loyalty: processing of personal data shall favour the interests of the data subject and a reasonable expectation of privacy, which shall be understood as the level of confidence that any person deposits in another that the personal data exchange between them shall be processed as agreed between them in compliance with the Private Data Protection Law.

g Transparency: data controllers shall inform data subjects, by means of a privacy notice, about the personal data that will be subject to processing, and the purpose or purposes for the processing. With respect to sensitive personal data, the privacy notice shall expressly state that the information is of a sensitive nature.

h Responsibility: data controllers shall adopt the necessary measures to comply with all data protection principles during the processing of personal data, even if the processing is carried out by data processors or third parties. Therefore, a data controller shall ensure full compliance with the privacy notice delivered to the data subject by that data controller or by third parties with whom it has a legal relationship.

In addition to the aforementioned principles, all data controllers shall comply with the duties of security and confidence, which are also applicable to data processors and third parties receiving any personal data from a data controller, in which case the latter must verify that these duties are observed by the third parties concerned.

Data controllers shall implement appropriate organisational, technical and physical security measures to protect personal data against unauthorised damage, loss, modification, destruction, access or processing. These measures shall be at least equivalent to those implemented for their own confidential information.

Further, all personal data shall be kept confidential, even upon the termination of any relationship with the data subject.
Compliance

Even though the INAI has ex officio authority to supervise compliance with the Private Data Protection Law, to date, most proceedings to verify compliance have resulted from claims filed by data subjects, with the exception of certain ex officio proceedings that have resulted from newspaper reports or claims filed by data subjects.

ii General obligations for data handlers

Although a data controller must comply with each and all of the principles described above (see Section III.i), the most basic obligations imposed on data controllers are mainly the drafting of privacy notices and making these available to data subjects, as well as appointing someone or creating a department in charge of handling all affairs related to data protection, including, without limitation, processing a response to any request submitted by a data subject.

The drafting and delivery of the privacy notice to a data subject constitutes a key factor in complying with the principle of transparency described above and, therefore, there are no exemptions to the same. As a result of the above, the privacy notice must be drafted complying with strict standards and requirements stipulated in the Private Data Protection Law, its Regulations and, particularly, the Guidelines. There are three types of privacy notices whose general characteristics, terms and conditions are as follows:

a full: a full privacy notice must be used when the personal data is personally collected from a data subject, and must contain all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines;

b simplified: a simplified privacy notice may be used when the personal data are collected directly but using remote means from the data subject and must contain all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines; and

c abbreviated: an abbreviated privacy notice may be used when personal data is directly obtained from a data subject by printed means and when the personal data collected is minimal. It must be drafted in accordance with Article 28 of the Regulations and Guideline 38 of the Guidelines.

In spite of the obligations provided in the Private Data Protection Law, data controllers must bear in mind that the main restrictions on commencing the processing of personal data consist principally of the need to make the privacy notice available to the data subject and also to obtain consent for the processing (except when the requirement for consent is exempted). Consent for processing any personal data must be obtained upon the collection of the personal data if the collection is made personally or directly from the data subject, or before any processing if personal data was not collected by the data controller directly from the data subject.

When drafting the privacy notice, data controllers must identify the different uses intended for the personal data, and also distinguish those uses required for the legal relationship between the data controller and data subject (necessary purposes) from those that are not (secondary purposes). This requirement is important considering that a data subject may choose to reject (or in the future withdraw consent for) processing for those secondary purposes without affecting his or her relationship with the data controller.
Data subjects also have the following rights, which are meant to secure protection of personal data (the ARCO rights):

- **Access**: a data subject is entitled to access his or her personal data held by a data controller, as well as to know the privacy notice to which processing is subject;

- **Rectification**: a data subject is entitled to rectify his or her personal data when it is inaccurate or incomplete;

- **Cancellation**: a data subject shall always be entitled to cancel his or her personal data. The cancellation of personal data implies that the information shall be kept by the data controller as long as prescribed in the applicable statute of limitations, with the sole purpose of determining possible responsibilities deriving from the processing. Once that time has elapsed, the data controller shall delete the corresponding personal data; and

- **Opposition**: a data subject shall always be entitled, with legal cause, to oppose the processing of his or her data. If a data subject does so, the data controller shall not be entitled to process the data concerning that data subject.

Notwithstanding the above, and in addition to the ARCO rights, the data subject shall also be entitled to withdraw consent (withdrawal), either in whole or in part, with respect to the processing of personal data, and may limit the use or divulgement of personal data (data limitation), and, collectively with the ARCO rights and the right of withdrawal (data claims), by opting out mechanisms or enrolling in lists kept by the data controller, or of Profeco or Condusef, of those data subjects unwilling to receive marketing communications. The data controller shall describe the means available to the data subject to exercise any of the data claims. Data claims shall be exercised free of charge, unless the data subject exercises the same claim to access personal data within a period of 12 months, in which case the data controller may charge a fee that shall not exceed three times the unit for measure and update (UMA) in force. Unfortunately, the creation of awareness in Mexico regarding the protecting of personal data is still a major challenge, considering that the lack of knowledge (and, in some cases, interest) together with the degree of specialisation of this matter may be delaying proper compliance with the Private Data Protection Law. Many data controllers are still gaining interest and experience in these matters, which has caused inadequate implementation of privacy notices, since this requires adequately mapping all data being processed to assess all implications. It is still common to see data controllers drafting their privacy notices without considering whether they are in fact processing any personal data, and to what extent.

### iii Specific regulatory areas

Notwithstanding the fact that the Private Data Protection Law is applicable to all private parties processing personal data, with certain exceptions, and that the Governmental Data Protection Law is enforceable in respect of any processing carried out by public agencies, Mexican Official Standard NOM-004-SSA3-2012 regarding medical records is currently the only extant industry- or sector-specific legal framework – despite the idea fostered by the Private Data Protection Law that laws or regulations applicable to specific sectors or industries should be enacted. Among other relevant provision made by this standard, it defines the concept of ‘clinical records’ and imposes obligations of confidentiality in respect of these records; health providers and establishments that gather, manage and store clinical records are required to implement all measures necessary to maintain this confidentiality (e.g., password-protected firewalls).
iii Technological innovation and privacy law

Technological innovations pose a challenge under the Private Data Protection Law, as this area is broadly and scarcely regulated, with no specific rules applicable to processing affected by such developments. Concepts such as ‘big-data analytics’ and the ‘internet of things’ have not yet been defined under the Private Data Protection Law or other applicable data protection legislation. However, processing of personal data using any technological innovation (including the use of remote or local communications media or any other technology) is governed by the Private Data Protection Law, therefore the challenge lies in determining the degree of applicability of that Law, given that the data subject must be informed of the processing. When using remote or local communications media or any other technology, notification must be given to the data subject through a visible communication or warning about the use of those technologies to process his or her personal data, and about the manner in which the technological mechanism may be disabled (unless its use is fundamental for technical reasons). This information must be also included in the full privacy notice, clearly identifying the personal data being collected by that means, as well as the purpose of the collection.

IV INTERNATIONAL DATA TRANSFER

Mexico is party to several international organisations (such as APEC – the Asia-Pacific Economic Cooperation – and the Organization of American States) that aim to protect personal data being transferred within their respective regions, whether domestically or internationally; however, to date, Mexico has signed no international treaties or conventions on this matter.

Under the Private Data Protection Law, an international communication of personal data originating from a data controller subject to the Private Data Protection Law may be deemed either a ‘transfer’ or a ‘remittance’, depending on the purpose for communicating the data and the recipient of the same. Each of these communications must meet specific requirements, which are described below.

i Transfer of personal data

A transfer is any communication of personal data by a data controller to any private or public entity different from the data subject or the data processor. In this regard, any transfer of personal data must be consented to by the data subject concerned, except where exempted pursuant to Article 37 of the Private Data Protection Law; the transfer must be notified to the data subject by means of a privacy notice and limited to those purposes justifying the transfer.

A data controller would be able to transfer personal data without the consent of a data subject if the transfer is:

a stipulated by a law or treaty to which Mexico is party;

b needed for prevention of illness or medical diagnosis, healthcare assistance, medical treatment or management of health services;

c made to holding companies, subsidiaries or affiliates under common control of the data controller who operate under the same processes and internal policies;

d required by an agreement entered into or to be entered into between the data controller and a third party in the interest of the data subject;

e necessary or legally required to protect the public interest or the prosecution or enforcement of justice;
required for the acknowledgment, exercise or defence of a right in a judicial proceeding; or

necessary for the preservation of, or compliance with, a legal relationship between the data controller and the data subject.

Any international data transfer shall be evidenced by an agreement or any other document whereby the third party assumes the same data protection obligations undertaken by the data controller and the conditions for processing as consented to by the data subject as detailed in the corresponding privacy notice. International data transfers do not need the approval of the INAI or any other Mexican regulatory agency to be completed and there is no need to submit standard contractual clauses or comparable instruments to any of them; however, a data controller may seek, at its sole discretion, the opinion of the INAI on compliance with the requirements before completing a transfer of personal data.

**Remittance of personal data**

A remittance is any communication of personal data made by a data controller to an individual or legal entity that is unrelated to the data controller with the purpose of conducting any processing on behalf of the data controller.

A remittance does not need to be notified to a data subject by means of a privacy notice, nor does it require the consent of the data subject. However, to carry out the remittance, a data controller and data processor shall enter into a certain agreement with the purpose of evidencing the existence, scope and content of the relationship, which should be consistent with the privacy notice delivered by the data controller to the relevant data subject.

Under non-Mexican laws, certain restrictions or requirements may have to be fulfilled prior to completion of an international transfer of personal data. For example, Mexico has not applied for, and therefore has not been recognised by, the European Commission as a third country providing adequate data protection to facilitate personal data transfers to countries within the EU.

**COMPANY POLICIES AND PRACTICES**

The following are among the security measures data controllers must implement:

- carry out data mapping to identify the personal data that are subject to processing and the procedures involving in the processing;
- establish the posts and roles of those officers involved in the processing of the personal data;
- identify risk and carry out a risk assessment when processing personal data;
- implement security measures;
- carry out a gap analysis to verify those security measures for which implementation is still pending;
- develop a plan to implement those security measures that are still pending;
- implement audits;
- conduct training for those officers involved in the processing;
- have a record of the means used to store personal data; and
- put in place a procedure to anticipate and mitigate any risks arising from the implementation of new products, services, technologies and business plans when processing personal data.
VI  DISCOVERY AND DISCLOSURE

Data controllers are obliged to disclose personal data in the event that there is a binding and non-appealable resolution from a competent Mexican authority. A data subject's consent for the processing of personal data shall not be required to the extent that the processing is meant to comply with a resolution from a competent Mexican authority. The Constitution grants all individuals the fundamental right to protect their personal data, as well as the right to access, rectify, cancel and oppose any processing of the same. It should be noted that the Constitution recognises that this right is not without limit; therefore, those principles protecting personal data are subject to certain exceptions for national security, public policy, public security and health, or to protect third-party rights.

Transfers of personal data for legal proceedings or investigations in other countries shall always be carried out in compliance with the Private Data Protection Law and through a letter rogatory following the adequate diplomatic or judicial channels. Data controllers should always analyse whether the privacy notice was disclosed to the data subject, whether the consent is required or exempted and was properly granted, and whether the transfer is limited to those purposes used to justify it. Additionally, the data controller and the relevant authority should enter into an agreement or any other document, as described in Section IV.

VII  PUBLIC AND PRIVATE ENFORCEMENT

i  Enforcement agencies

Initiation of proceedings

The INAI takes charge of data protection proceedings (DPPs) and of compliance-verification proceedings (VPs).

DPPs are intended to resolve claims filed by a data subject or his or her legal representative alleging that a data controller has failed to attend to a claim exercising the data subject’s ARCO rights or when the resolution of the data controller does not satisfy the data subject.

VPs may be commenced ex officio by the INAI or at the request of a party. An ex officio VP will take place following a breach of a resolution issued in connection with a DPP, or if a breach of the Private Data Protection Law is presumed to be founded and substantiated by the INAI. During a VP, the INAI shall have access to the information and documentation deemed necessary, in accordance with the resolution originating the verification.

Penalties

In the event that the INAI becomes aware during a DPP or VP of a presumed breach of the Private Data Protection Law, a proceeding to impose penalties will commence assessing the infringement. The available penalties include the following:

- a warning issued by the INAI urging a data controller to comply with the data subject’s demands. Note that this course of action is limited to certain types of infringement;
- fines representing an amount of between 100 and 320,000 times the UMA, which is published by the National Institute of Statistics and Geography, which will be determined based on the nature of the infringement; and

---

2 Between 7,549 and 24,156,800 Mexican pesos in 2017.
imprisonment for up to three years in certain cases, such as when someone authorised to process any personal data causes a security breach in relation to the data under his or her control with the purpose of obtaining a gain; or imprisonment for up to five years when someone processes personal data with the intention of obtaining a gain by deceiving, or taking advantage of the error of, a data subject or the person authorised to transfer any personal data.

The penalties set out in (b) and (c) above may be doubled if the infringement involves sensitive personal data. Although the Private Data Protection Law does not entitle a data subject to receive any indemnification in light of damage suffered because of a data controller’s breach, it does acknowledge that any of the fines or penalties indicated above would be imposed against a data controller without prejudice to any liability that the data controller may have in civil and criminal law.

When assessing the fine or penalty to be imposed, the INAI would consider:

- the nature of the personal data;
- the inappropriateness of the failure to comply with the claim of the data subject;
- whether the action or omission was deliberate;
- the economic capacity of the data controller; and
- any reoccurrence of the breach.

Data controllers may challenge these sanctions or fines by means of a nullity claim before the Federal Court of Tax and Administrative Justice.

In addition, Profeco and Condusef are entitled to verify the adequate use of consumer information. If either of them finds that a corporation is engaging in unsolicited marketing to a customer enrolled in the Public Registry of Consumers or the Public Registry of Individual Users, or that it has used consumers’ data for a purpose other than marketing, the following shall apply: as of 2017, Profeco may impose fines of up to 1.56 million Mexican pesos; or Condusef may impose fines of up to 2,000 times the UMA in force.3

In recent years, the INAI has fined, inter alia, financial institutions, telecom companies and healthcare providers. The most significant fines imposed by the INAI so far are discussed below. However, most of these fines have been challenged by the data controllers concerned and the proceedings are pending resolution.

**Tarjetas Banamex**

A fine of 9.8 million Mexican pesos was imposed on Tarjetas Banamex, SA de CV SOFOM, ER (Tarjetas Banamex) on the grounds that Tarjetas Banamex personnel made telephone calls to collect an unpaid balance but to a telephone number belonging to a data subject that was different from the cardholder in question, and failed to allow the data subject to rectify and cancel his personal data stored with Tarjetas Banamex.

---

3 146,080 Mexican pesos in 2016.


**Telcel**

A fine of 10.2 million Mexican pesos was imposed on Radiomóvil Dipsa, SA de CV (Telcel). Telcel personnel had made calls to collect unpaid balances from individuals who were on a frequently dialled-number list of persons owing money to Telcel, and divulged to them the amount owed without the express consent of the data subject.

**Banorte**

A fine of 32 million Mexican pesos was imposed on Banco Mercantil del Norte, SA, Institución de Banca Múltiple, Grupo Financiero Banorte (Banorte). Banorte collected sensitive personal data without the consent of the data subject and stored the data without a legal justification in breach of the principles of information, proportionality and legality, as it failed to deliver a privacy notice to the claimant and processed personal data of the husband of the claimant that was not necessary, adequate or relevant for the purpose of the data collection.

**ii Recent enforcement cases**

A fine of 35,050 Mexican pesos was imposed on a fitness club. The INAI’s decision to fine the fitness club was based on the following arguments:

- fingerprints are biometric data and constitute sensitive personal data, therefore the fitness club collected the data without the written consent of the data subject;
- the fitness club privacy notice did not comply with the Private Data Protection Law; and
- the fitness club processed personal data from the claimant in breach of the principles of information, responsibility and legality, since the fitness club failed to deliver its privacy notice to the claimant, did not adopt adequate security measures and processed personal data in contravention of the Private Data Protection Law.

**iii Private litigation**

The Private Data Protection Law makes no provision regarding remedies or financial recovery for the data subject as a result of a breach of data protection rights; however, data subjects are entitled to file a claim before the civil courts to seek indemnification resulting from moral damage. We are not aware of any claims of this nature. The first chamber of the Mexican Supreme Court has issued certain groundbreaking, non-binding court precedents resolving that, when awarding damages, courts and judges shall considering aggravating factors, such as the degree of responsibility, to determine a fair indemnification, thereby openly recognising concepts such as 'punitive damages', which were not developed in court precedents.

**VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS**

The Private Data Protection Law is applicable to:

- data processors not located in Mexico, but that process personal data on behalf of data controllers located in Mexico;
- data controllers that are not located in Mexico, but that are subject to Mexican laws as a result of an agreement or in terms of international laws; or
- data controllers using means located in Mexico (even if they are not established in Mexico), except if those means are merely for transit purposes, without involving the processing of personal data.
As a result of the above, foreign companies must always analyse whether their activities, or the activities of their affiliates, would result in the application of the Private Data Protection Law.

Foreign companies have also faced certain challenges considering that, under the premise that privacy notices should be simple and easy to understand, the INAI has been reluctant to accept privacy notices issued by multiple data controllers, even if they are part of the same corporate group.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity is broadly addressed within the Private Data Protection Law and its Regulations, by establishing that all private entities processing personal data, and data controllers in particular, shall have adequate physical, technical and organisational measures to prevent any personal data breach. It should be noted that the Private Data Protection Law and its Regulations do not attempt to impose a catalogue of security measures to be adopted by those bound by them, but rather outlines general principles applicable to security measures that shall be implemented by those processing personal data. In that spirit, the INAI has issued certain documents in an attempt to simplify the implementation of security measures, such as:

a the Recommendations on Personal Data Security outlining the minimum actions needed to securely process personal data;
b the Methodology for Analysing Risk to assess the risks when processing personal data;
c the Guide to Implementing a Personal Data Security Management System to establish security measures based on the cyclic model of ‘planning, doing, checking and acting’; and
d the Guide on Personal Data Security for Micro, Small and Medium-Sized Businesses, which guides such companies in compliance with the Private Data Protection Law and its Regulations with respect to security measures and the implementation of a personal data security management system.

A data controller must notify each data subject upon confirmation that a data breach has occurred, once it has taken any actions intended to assess the magnitude of the breach. The notice shall contain at least the nature of the incident, the personal data affected, advice on the actions that may be adopted by the data subject to protect his or her interests, the remedial actions that were immediately carried out and the means through which the data subject may obtain further information. In addition, the data controller would have to take corrective and preventive actions and improve its security measures to avoid the reoccurrence of the same breach.

The Private Data Protection Law and its Regulations do not oblige a data controller to notify the INAI upon the occurrence of a breach or of the measures taken by the data controller. However, failing to comply with any of the obligations mentioned above may constitute an infraction under the Private Data Protection Law that may result in the imposition of sanctions by the INAI.

X OUTLOOK

We are not aware of any intended amendments to the Private Data Protection Law since the previous edition of this publication.
Chapter 19

NIGERIA

Folabi Kuti, Ugochukwu Obi and Seth Azubuike

I OVERVIEW

Nigeria does not have an omnibus law or comprehensive piece of legislation that provides broad data protection principles covering all sectors engaged in processing of personal data. Unlike countries in Europe that favour the comprehensive or governmental regulatory approach to data protection, Nigeria seems to favour a sectoral model of data protection regulation.

Notwithstanding the above, Section 37 of the Constitution of the Federal Republic of Nigeria (CFRN) 1999, provides for citizens’ right to private and family life: ‘the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected’.

Although the CFRN sets the background for the protection and safeguard of citizens’ privacy, it does not specifically define the scope of the term ‘privacy’. That said, certain sectoral regulations on data protection are outlined briefly below.

Recently, the National Assembly passed into law the Credit Reporting Act 2017. The purpose of the Act is to promote access to accurate, fair and reliable credit information and to protect the privacy of such information.

The Credit Reporting Act further ensures data protection and safeguards the rights of data providers by stipulating the following:

a a requirement for a permissible purpose for collecting credit information;

b the confidentiality rights of data subjects and credit information providers; and

c the responsibilities of credit information users, among other things.

There is also some degree of data protection in the Nigerian telecommunications sector. Because of the increasing public demands for regulators to protect the personal data of telephone service subscribers in Nigeria, the Nigerian Communications Commission (Regulation of

1 Folabi Kuti is a partner, Ugochukwu Obi is a senior associate and Seth Azubuike is an associate at Perchstone & Graeys.


3 Section 1(b) of the Credit Reporting Act.

4 See Sections 5, 7, 8, 9, 11 and 12 of the Credit Reporting Act, available at www.nassnig.org/document/download/8430.
Telephone Subscribers) Regulations 2011 (the RTS Regulations)\(^5\) afford some protection of the personal data collected, collated, retained and managed by telecommunication operators and independent registration agents under the RTS Regulations.\(^6\)

In 2007, the Nigerian Communications Commission (NCC)\(^7\) issued the Consumer Code of Practice Regulations (the NCC Consumer Code). The purpose of the NCC Consumer Code is, among other things, to set out the responsibilities of a licensee (service provider) regarding the protection of individual consumer information.\(^8\) The NCC Consumer Code requires the licensee to protect data collected from consumers, to maintain a good data protection policy and to ensure compliance with the NCC’s data protection policy (see Sections V–VII).

Apart from sectoral provisions, there are laws that address a subject or an objective rather than a sector, and that make provision for data protection or privacy; for example, the provisions of the Freedom of Information Act No. 4 of 2011 (the FOI Act). While its general objective is to make public records and information accessible, the FOI Act makes an exception for personal information.\(^9\) Further, under the Child Rights Act No. 26 of 2003 (the Child Rights Act)\(^10\) data protection and privacy standards apply to information relating to a child.

There are also other cross-sectoral enactments that provide data protection and privacy standards. These enactments affect the country’s social, political and economic institutions. One example is the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (the Cybercrimes Act), the purpose of which is to regulate the use of internet and computer-based information and to prevent crime in these areas. It further establishes specific penalties for offences related to cybercrime. Although the term ‘cybercrime’ is not defined in the Act, it identifies certain offences, such as cyberstalking and unlawful access to a computer or information.\(^11\)

The approach to implementation of data protection policies is usually through a framework put in place by the government regarding such policies. For instance, upon enactment of the FOI Act, the Nigerian government mapped out a schedule to create public awareness and ensure participation by members of the public in implementing the Act. In addition, data privacy and cybersecurity law has been implemented through regulatory compliance checks and the use of task forces.\(^12\)

Non-governmental organisations (NGOs) and advocacy groups are also involved in the development of privacy policies. NGOs have, through constructive actions, supported


\(^{6}\) RTS Regulations, ss. 7–10 (especially s. 9).

\(^{7}\) The NCC exercises, inter alia, regulatory oversight functions in the telecommunications sector in Nigeria pursuant to the Nigeria Communications Commission Act 2003.


\(^{9}\) Section 14 of the FOI Act.


\(^{12}\) State governments mostly create task-force offices to monitor citizens’ compliance with regulations. For example, in Lagos State, there are task-force officials, comprising law enforcement officers and other trained persons, who carry out searches in strategic areas to ensure that cybercrimes are not being perpetrated.
the implementation, and helped to increase awareness, of some of these laws. For example, the members of the National Youth Service Corp have facilitated public awareness of the FOI Act.\(^\text{13}\)

Furthermore, under Nigerian jurisprudence, data protection and privacy policies are often discussed in relation to the regulatory and legal framework. Put simply, data protection and privacy are treated as coextensive in Nigeria. Consequently, as stated earlier, most sectoral or cross-sectoral legislation and regulations contain provisions on both privacy and data protection,\(^\text{14}\) with the effect of creating an implicit right of privacy for the individual and entitling the individual to seek remedies in the event of a breach of his or her data privacy.

In addition, privacy and data protection are designated as fundamental human rights in Nigeria.\(^\text{15}\) While freedom of expression is a constitutional right, allowing every citizen of right to hold his or her own opinions, and to own any means of disseminating information, this is qualified in that the exercise of this right is limited to what is allowed pursuant to other enactments in this area.\(^\text{16}\)

While there are a number of obligations established between the government and companies to ensure compliance with data protection and privacy policies, the government has constantly faced the dilemma of whether to take further measures on privacy and data protection rights given the likelihood that certain issues may arise. Pursuant to the Companies and Allied Matters Act (CAMA),\(^\text{17}\) corporate bodies are requested to submit annual updates on the company’s affairs.\(^\text{18}\) While it is important for the government to protect data that is sensitive in relation to national security, this provision of the CAMA does not anticipate submissions of information on privacy and data protection. Consequently, corporate privacy obligations in Nigeria depend on companies’ privacy policies, which apparently vary from one company to the other.

Thus, the major distinction between government and corporate privacy obligations is that government is responsible for providing the regulations and guidelines relating to data protection and privacy standards in the various relevant sectors and the corporate bodies are responsible for ensuring that their privacy policies comply with those regulations and guidelines.

The Cybercrimes Act makes provision for lawful interception of data and any law enforcement agent or such other body as may be granted the power by a court of law may take steps to monitor, intercept or ask for records or data regarding communications between any persons. A specific law allowing for government surveillance called the Lawful Interception of Communications Regulations, made pursuant to the Nigerian Communications

---


\(^\text{14}\) The NCC General Consumer Code of Practice, Part VI – Protection of Consumer Information, Sections 34–38, which provide for the protection of consumers’ private information submitted to network providers.

\(^\text{15}\) Ezeadukwu v. Maduka (1997) 8 NWLR (Pt. 518) 635.

\(^\text{16}\) Section 39(3) of the CFRN 1999 (as amended).

\(^\text{17}\) Companies and Allied Matters Act 1999, Cap. C20, LFN 2004.

Commission Act 2003, is still at the draft stage.\(^{19}\) This draft law has, however, been the subject of serious opposition in recent times.\(^{20}\) Also, the CFRN allows the government to derogate from citizens’ right to privacy for certain reasons.\(^{21}\)

In addition, and notwithstanding efforts by the government to curb breaches of data protection and privacy rights, there have been several concerns raised over the issue of online fraud in Nigeria.\(^{22}\)

II THE YEAR IN REVIEW

In view of the recent growth in the use of data and emergence of information and communications technology in Nigeria, the need has manifestly arisen to develop further laws in this field and there have been several developments in this regard, including:

\(a\) the Credit Reporting Act was enacted;\(^{23}\) and
\(b\) the Electronic Transaction bill was passed by the Nigerian Senate.\(^{24}\)

Furthermore, following the global WannaCry ransomware attack, cybersecurity issues have been given greater priority in Nigeria. However, the National Information Technology Development Agency (NITDA) has clarified that Nigeria was largely unaffected by the aforesaid cyberattack.\(^{25}\)

That notwithstanding, Nigeria continues to suffer major data breaches or privacy incidents, including the following:

\(a\) hacker attacks on Nigerian financial institutions;\(^{26}\)
\(b\) the WannaCry attack and subsequent calls for sustained cybersecurity;\(^{27}\) and
\(c\) Nigerian hackers are reported to have stolen US$3 billion worldwide.\(^{28}\)

See Section X of this chapter for further analysis of the events that have happened in the year in view.

---

\(^{19}\) www.ncc.gov.ng/documents/328-lawful-interception-of-comunications-regulations/file. The bill has passed its first reading on the floor of the two houses.

\(^{20}\) www.vanguardngr.com/2015/07/ncc-stakeholders-disagree-on-call-interception-licensing-regulation-draft/.

\(^{21}\) Section 45 of CFRN as amended 2010.

\(^{22}\) http://tinyurl.com/y9qftlzp.


\(^{27}\) See footnote 25.

\(^{28}\) www.vanguardngr.com/2017/06/nigerian-hackers-steal-3b-worldwide-reports/.
III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

As stated above, regulatory agencies in each sector and certain other bodies empowered to do so issue sector-specific data privacy regulations. Privacy and data protection-related legislation and regulations include:

a The CFRN (as amended) – while there is no omnibus law in Nigeria for data protection and cybersecurity, Section 37 of the CFRN provides a basis upon which subsequent laws and regulations on data protection can be construed.

b The Nigeria Communications Commission Act 2003 (the NCC Act) empowers the NCC to regulate the activities of operators (including regarding protection of data) in the information and communications sector.

c The NCC Consumer Code, Part VI, which was established in 2007, regulates management or protection of customers’ information or data.

d Regulation 9 of the RTS Regulations governs data protection and confidentiality, and requires network operators to manage and protect data received from customers.

e The FOI Act, the objective of which is to ensure that the public is not denied access to public information. However, the FOI Act sets out private information as an exemption (although it may be requested by the public), thereby ensuring privacy of personal information.

f The Credit Reporting Act 2017 provides for protection of data received by financial institutions from borrowers through credit bureaux.

g The Cybercrimes Act, the purpose of which is to protect critical national infrastructure, to regulate the use of internet and computer-based information, and to prevent crime connected thereto.

In addition, some of the above-mentioned pieces of legislation define the scope of what may be classified as personal information, data, a database, interception, etc.

To avoid breaches or violations, the activities of data handlers in the various sectors are generally guided by the laws or regulations. For instance, under Section 35 of the NCC Consumer Code, the NCC conducts quarterly compliance monitoring and enforcement, and releases reports to this effect.

Consequently, Nigerian law allows an aggrieved data subject to claim damages or redress in respect of an act or omission of a data handler that has occasioned injury to the data subject either physically or otherwise. However, where the act or omission is criminal in nature, proof of injury to the person of the victim will not be required to impose penalties or sanctions against the erring person.

30 FOI Act, Cap. I14 No. 4 of 2011.
31 See Section 31 of the FOI Act and Section 58 of the Cybercrimes Act respectively.
33 For example, any act or omission contrary to the Cybercrimes Act.

© 2017 Law Business Research Ltd
ii  General obligations for data handlers

In a bid to adopt the trend for information and communication technology, most regulatory authorities in Nigeria have employed an online registration procedure. In most cases, customers are required to register online and also upload certain information, which has to be updated frequently. Among these authorities are:

a  the Corporate Affairs Commission;\(^{34}\) and
b  the Department of Petroleum Resources.\(^{35}\)

Laws or regulations create obligations for data handlers; for instance, in most cases, for data or information to be obtained, the data handler is expected to request the person seeking information to state reasons or the purpose for requesting the information. Under the Freedom of Information Act, for example, any person seeking to obtain information is required to make a formal application stating the grounds upon which the information should be released.

However, while levels of awareness are not high in respect of rights under the various provisions for data protection in Nigeria, it has become important that data handlers take reasonable care in managing information received from data subjects, as any negligent actions or omission in this regard may attract legal actions against the data handler.

iii  Technological innovation and privacy law

Developments in information and technology have made storage and usage of sensitive or private information a valuable commodity that can be easily abused or misused, and while various sectors in Nigeria have benefited in this regard, they have also faced challenges. The financial sector in Nigeria, for instance, undoubtedly involves itself with the accumulation and storage of high volumes of personal and financial data of bank customers in respect of numerous financial activities but especially electronic banking transactions. Therefore, the risk of banks using the information derived and stored on their electronic banking platforms for commercial purposes remains high. To ensure the protection of bank customers’ rights in electronic banking transactions, the Central Bank of Nigeria (CBN)\(^{36}\) in August 2003 issued its Guidelines on Electronic Banking in Nigeria. These Guidelines sought to address the following key issues:

a  information and communications technology standards on security and privacy;
b  monetary policy;
c  legal guidelines on banking regulations and consumer rights protection; and
d  regulatory and supervisory issues.\(^{37}\)

---

\(^{34}\) The Corporate Affairs Commission is a body empowered under the CAMA to formulate, incorporate, regulate the management and eventual winding-up of a company (http://new.cac.gov.ng/home/).

\(^{35}\) The Department of Petroleum Resources is a government establishment under the ministry of petroleum, to manage all activities in respect of crude and petroleum (http://recruitment.dpr.gov.ng/login).

\(^{36}\) CBN exercises, inter alia, regulatory oversight functions over banks and other financial institutions in Nigeria.

\(^{37}\) It has been advocated in several fora that the Guidelines on Electronic Banking in Nigeria should be revised as they are slightly outdated, and there have been significant developments in electronic banking since they were initially developed (especially with respect to protection of electronic data).
Furthermore, the CBN Guidelines for Card Issuance and Usage 2014 place a heavier burden on banks to guarantee the security of cards issued to cardholders. It states that “The security of the payment card shall be the responsibility of the issuer and the losses incurred on account of breach of security or failure of the security mechanism shall be borne by the issuer, except where the issuer establishes responsibility for the security breach on the part of the card holder.”\(^\text{38}\) It further provides that “Issuers should ensure that the process of card issuance is completely separated from the process of PIN issuance, and done in accordance with best practices thus minimizing the risk of compromise.”\(^\text{39}\)

**IV  INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION**

The Nigerian government has constantly reiterated its commitment to ensuring localisation of data.\(^\text{40}\) In 2011, the CBN introduced a measure that required all point-of-sale and ATM transactions to be processed locally. Under no circumstances are these transactions to be processed outside Nigeria.\(^\text{41}\) Subsequently, in 2013, NITDA issued the Guidelines for Nigerian Content Development in Information and Communications Technology (the NITDA Guidelines),\(^\text{42}\) which introduced several restrictions on cross-border data flows and mandated that all data of government ministries, departments and agencies (MDAs) should be stored and hosted locally in Nigeria. The Office for Nigerian Content Development, a subsidiary of NITDA, was also established to develop Nigeria’s indigenous information and communication technology (ICT) industry and enforce the Guidelines. The object of the Guidelines is to encourage development of local content in Nigeria and ensure that Nigerians are actively involved in the ICT industry, and also to put in place measures to check the activities of companies in the industry.

NITDA also issued in 2013 the National Information Systems and Network Security Standards and Guidelines,\(^\text{43}\) establishing minimum standards in seven areas: categorisation of information; minimum security requirements; intrusion detection and protection; protection of critical information infrastructure (CII); securing public web services; system firewalls; and cyber-forensics. Those organisations implementing the guidelines must ensure they ‘meet the minimum security requirements in this standard by selecting the required security controls and assurance requirements as described by this document’.

As stated above, the discussed regulatory provisions restrict illegal access to information and data, except where permission is properly obtained, such as upon formal application to the necessary regulatory body or where a court has given an order directing the authority or institution in charge of the information to release or submit the information.

\(^{38}\) Para. 3.21 of the CBN Guidelines for Card Issuance and Usage.

\(^{39}\) Para. 3.22 of the CBN Guidelines for Card issuance and Usage.


V COMPANY POLICIES AND PRACTICES

Generally, policies of companies in Nigeria with respect to protection of company data are usually decided and approved by the management of the company (usually its board of directors), which derives its powers from the CAMA.\(^{44}\) However, the CAMA does not expressly stipulate a mechanism whereby companies handling personal information can effectively protect such data against its misuse. The implication of this is that the CAMA, to a large extent, allows companies to develop and implement their own policies, ideas or mechanisms as to the collection, processing, use, storage, retention or deletion of personal information in their possession.

Company policies vary from one company to the other. This is because the appropriate security measures for each company depend on the nature of the company’s operations, as there is no one-size-fits-all approach to securing personal data. That notwithstanding, the terms of every internal company policy regarding protection of personal data must fall within the provisions of the relevant regulations for the sector in which the company operates. For instance, the NITDA Guidelines provide protective measures for ICT companies to adopt to protect consumer data in their custody. These measures include hosting all subscribers and consumer data locally within the country and hosting their websites on the .ng top-level domain.\(^{45}\) In addition, the NITDA Guidelines mandate that all network companies must maintain and audit protocols for all services involving citizens’ data, corporate data and data held by MDAs. The NITDA Guidelines also vest consumers with the right to delete their personal information, data and other records on any service to which they are subscribed.\(^{46}\)

Furthermore, the NCC Consumer Code expressly provides that any telecommunication company that collects information on individual consumers shall adopt and implement a policy regarding the proper collection, use and protection of that information, and the policy shall be made available in an accessible and easy-to-read manner, including as specifically directed by the NCC from time to time.\(^{47}\)

In general, most companies employ physical, technical and administrative security measures to reduce the risks of loss, misuse, unauthorised access, disclosure and alteration of customers’ data held by them. Physical measures put in place by companies may involve assigning the responsibility of protecting and accessing the data collected to a senior officer, usually designated as the information security officer. Furthermore, the use of passwords, cookies, data encryption measures and advanced technologies are all measures geared towards securing and safeguarding all and any data collected by these companies.

VI DISCOVERY AND DISCLOSURE

Discovery and disclosure of information usually happen when personal information about consumers is made public without their consent. However, the imposition of a duty of data confidentiality on companies in Nigeria remains a major way of curtailing the misuse or

\(^{44}\) Companies and Allied Matters Act 1999, Cap. C20, LFN 2004.
\(^{45}\) 12.1 NITDA Guidelines.
\(^{46}\) 13.1(3), (5) NITDA Guidelines.
\(^{47}\) Sections 36 and 37 of the NCC Consumer Code; see footnote 8.
undue disclosure of private or personal information. To regulate data disclosure or transfer outside Nigeria, sectors have introduced guidelines or regulations (or a combination of these) in this regard, such as the RTS Regulations, introduced by the NCC in 2011.

The RTS Regulations provide that no subscriber’s information shall be transferred outside the Federal Republic of Nigeria without the prior written consent of the NCC. It further provides that the release of personal information to security agents shall only be done in accordance with the provisions of the NCC Act, the RTS Regulations and any guidelines or instrument issued from time to time (and in a format to be determined) by the NCC. The implication is that to obtain any personal information from telecommunication companies operating in Nigeria requires the prior approval of the NCC.

Furthermore, the NCC Consumer Code also provides that the collection and maintenance of information about consumers shall not be transferred to any party except as permitted by the terms and conditions agreed with the consumer, and also with the approval of the NCC, or as otherwise permitted or required by other applicable laws or regulations.

The Credit Reporting Act also restricts the purposes for which credit information may be accessed. Information provided or received can only be accessed for what is termed ‘permissible purposes’, among which is compliance with any court order to provide information or where a person is required by an applicable law to provide credit information in respect of any other person or in compliance with the directive of a regulatory authority or public body to provide credit information.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The NCC Act places the responsibility of the enforcement of data protection on the NCC, which it undertakes by making and enforcing regulations pursuant to its powers of investigation and intervention under the NCC Act. In addition, the NCC is empowered to conduct quarterly audits, inspections and monitoring of licensed telecom operators to ensure compliance with its codes and regulations.

With reference to matters involving information technology, NITDA is the foremost agency in Nigeria. The NITDA Act mandates NITDA to create a framework for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of ICT practices, activities and systems in Nigeria. NITDA also plays an enforcement role. To ensure effective enforcement, pursuant to the NITDA Guidelines, a breach of the provisions of the NITDA Guidelines shall be treated as a breach of the NITDA Act.

Furthermore, the Cybercrimes Act, which was enacted to provide an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria and to promote

---

48 Section 10 of the RTS Regulations.
49 Section 34(2) of the RTS Regulations.
50 Section 55 of the NCC Consumer Code.
52 See footnote 42.
cybersecurity and the protection of computer systems and networks, data and computer programs and privacy rights, by virtue of its Section 41 empowers the Office of the National Security Adviser (ONSA) to coordinate activities of all other security agencies with respect to the administration of the provisions of the Act and to coordinate Nigeria’s involvement in international cybersecurity cooperations to ensure the integration of Nigeria into global cybersecurity frameworks. The Attorney General of the Federation also bears the responsibility for cybersecurity matters and for ensuring the effective prosecution of cybercrimes.

ii Recent enforcement cases

In recent times, enforcement actions undertaken by agencies such as the NCC have primarily centred on regulatory compliance with the applicable laws and regulations rather than on breaches of data protection requirements.

On 20 October 2015, the NCC imposed a fine of 1.04 trillion naira on MTN for infraction of the provisions of the RTS Regulations. The company was fined for refusal to deactivate a total of 5.2 million unregistered SIM cards on its network within the prescribed deadline. After nearly six months of negotiation, however, both sides agreed that MTN should pay a fine of 330 billion naira, reduced from the initial fine of 780 billion naira. In light of the severity of the fine, the NCC, in collaboration with the federal government, agreed to spread the payments of the fine over six tranches, after the initial 50 billion naira was paid.

In its Compliance Monitoring and Enforcement Report (Quarter 1 – 2017), the NCC stated that its attention was drawn to some alleged cases of unauthorised subscription to mobile value-added services (VAS) by some telecommunication companies. The operators have since been directed to immediately stop VAS provision to the concerned subscribers and to submit the call date records for the NCC to determine further enforcement action regarding the matter.

iii Private litigation

The right to privacy is a fundamental right embodied in the CFRN. Where there is a breach or attempts to breach this right, the individual can seek a remedy under the Fundamental Right Enforcement Procedure Rules against the infringer. The remedies available for the individual include damages. However, the individual cannot obtain an injunction restraining a data collector from the collection of data. This is in view of the fact that data handlers in Nigeria are by law allowed to engage in data collection in their day-to-day activities.

Overall, private litigation on data protection and privacy are not very common in Nigeria and, notably, the responsibility to prove an incidence of breach of duty of care and resulting loss or damage lies with the individual claiming that his or her personal data has been breached or compromised.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The applicability of data protection or privacy laws to companies in Nigeria is predicated on whether the company operates in Nigeria and deals with the personal information of data subjects resident in Nigeria or who, if not resident in Nigeria, have their information hosted by that company in Nigeria.

Consequently, multinationals who have a presence in Nigeria will be required to comply with the laws on data protection.\(^{54}\) The NITDA Guidelines make salient provisions for multinationals, which they define as a firm that is registered in more than one country or that has operations in more than one country.\(^{55}\)

Specifically, the NITDA Guidelines stipulate that ICT companies shall host all subscriber and consumer data locally within the country.\(^{56}\) Also, data and information management firms are mandated to host government data locally within the country and, where they want to host the data abroad, must seek approval from NITDA and the Secretary to the Government of the Federation.\(^{57}\)

Finally, MDAs had to ensure that all government data is hosted locally inside the country within 18 months of the publication of the NITDA Guidelines.\(^{58}\) Where a multinational is operating in Nigeria as an ICT provider or for the Department for Information on Markets and Financing, it must comply with the data localisation requirements and have all its data hosted in Nigeria.

IX CYBERSECURITY AND DATA BREACHES

The Cybercrimes Act provides for the prohibition, prevention, detection, response and prosecution of cybercrimes and for other related matters. The Cybercrimes Act criminalises attacks against information systems, such as attacks on computer systems or networks designated as CII.\(^{59}\)

Furthermore, the Cybercrimes Act introduced some significant offences relating to data protection, notably:

- unlawful access to a computer;
- unlawful interception of communications;
- unauthorised modification of computer data;
- system interference.\(^{60}\)

Other criminal offences that could be related to cybercrime were also criminalised, such as computer-related fraud, computer-related forgery, identity theft and impersonation, child

---

54 The NITDA Guidelines. See footnote 42.
55 3.0, NITDA Guidelines.
56 12.1(4), NITDA Guidelines.
57 14.1(2), NITDA Guidelines.
58 14.2(3), NITDA Guidelines.
59 S. 5, Cybercrimes Act.
60 Ss. 6–9, Cybercrimes Act.

© 2017 Law Business Research Ltd
pornography, cyberstalking, cybersquatting, cyberterrorism, and racist and xenophobic offences.\textsuperscript{61} Notably, under the Cybercrimes Act, legal entities can be held criminally liable for the above-mentioned offences.\textsuperscript{62}

The Cybercrimes Act is ground-breaking legislation in that, unlike prior legislation, it is the first to make omnibus provisions in relation to cybersecurity and data protection. For instance, the above-mentioned offences on data protection are not sector specific and apply across sectors.

Prior to the enactment of the Cybercrimes Act, the ONSA, which is in charge of developing cybersecurity policy for Nigeria,\textsuperscript{63} had, in 2014, issued the National Cybersecurity Policy. The Policy provides that the federal government shall create the Nigerian Computer Emergency Response Team (ngCERT),\textsuperscript{64} whose functions are to respond and assist in addressing issues relating to cybersecurity in federal government networks.

Furthermore, the CBN has issued the Nigeria Banking Industry IT Standards Blueprint, which contains compliance standards for banks upgrading their cybersecurity defences.

The agencies responsible for making cybersecurity policy and enforcement include the ONSA, the Federal Ministry of Justice, the Nigeria Police Force and the Economic and Financial Crimes Commission. The Cybercrimes Act mandates all law enforcement agencies to develop the requisite institutional capacity for effective implementation.

In addition, the ONSA is responsible for initiating, developing or organising training programmes for personnel charged with responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.\textsuperscript{65} Finally the Cybercrimes Act establishes the Cybersecurity Advisory Council, which is a joint body of all stakeholder agencies, whose function is to create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis. The Council is also mandated to provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cybersecurity in Nigeria.

X OUTLOOK

Privacy, data protection and cybersecurity issues are still evolving in Nigeria. In the few years since the revolution in Nigeria’s telecommunications industry, legislation on these issues has burgeoned. In the coming year, it will be interesting to see how the Credit Reporting Act 2017 (the Act) plays out in terms of applicability and enforcement. Fortunately, the Act, while paving the way for the growth of credit bureaux in Nigeria, has far-reaching provisions regarding the protection of data subjects’ information. It will be important to see how new businesses (and existing ones) handle the task of their protecting data subjects.

The foregoing projection is in view of the fact that Nigeria’s financial sector continues to be the sector hit hardest by cybercrime. According to the Nigeria Electronic Fraud Forum (NEFF) the financial sector lost 2.19 billion naira to fraudsters in 2016.\textsuperscript{66} Moreover, 2017 saw

\textsuperscript{61} Ss. 11–18, Cybercrimes Act.
\textsuperscript{62} S. 20, Cybercrimes Act.
\textsuperscript{63} ONSA, National Cybersecurity Policy, p. 8.
\textsuperscript{64} ONSA, National Cybersecurity Policy, p. 33.
\textsuperscript{65} S. 24(3), Cybercrimes Act.
the collapse of Nigeria’s largest ever cyber-Ponzi scheme, popularly referred to as MMM. As reported by the NEFF, about 11.9 billion naira was lost to this scheme. Despite this, there is no end in sight to these cyber-Ponzi schemes because of huge public participation. If schemes evolve and begin to use cryptocurrencies, which are still unregulated and owners’ identities are not traceable, the schemes may become more fraudulent. A committee has been set up by regulators to look at bitcoin and a preliminary position is expected soon to enable the crafting of a proper framework for regulating cryptocurrencies.

Furthermore, data, privacy issues remain a concern for the world at large. Recall when ransomware locked up and held for ransom companies’ data in May 2017. The malicious software affected about 300,000 computers in 150 countries. Several organisations in Nigeria were also hit by ransomware attacks in 2016 and 2017. Consequently, it is expected that outsourcing cybersecurity intelligence services will continue to grow as organisations that lack the required skilled resources and seek to cut the costs of setting up infrastructure will choose to outsource such services.

Finally, we expect the General Data Protection Regulation (GDPR) and the European Union’s response to risks linked with the increased role that technology now plays in daily life to have some significance in Nigeria’s space. This is because the GDPR, although an EU regulation, applies to any organisation, regardless of its physical location, so long as it collects the personal data of EU residents. A likely issue for Nigerian companies or organisations dealing with data of EU residents arises from the fact that the GDPR gives individuals the right to be forgotten, which means that when they terminate their relationship with an organisation they can exit with their personal data, and all personally identifiable information must be removed. Cybersecurity systems giant Fortinet reports that in addition to the impact on information and security technologies, GDPR compliance will require changes to some core business processes, including data processing workflows, organisational structures and even core business policies.

---

67 Mavrodi Mundial Moneybox.
68 This will include supranational and international organisations with country offices in Nigeria.
Chapter 20

POLAND

Anna Kobylańska and Marcin Lewoszewski

I OVERVIEW

When it comes to protection of privacy and personal data, Poland has followed the EU standards and laws for many years and it seems likely that the country will prepare its legal framework for the General Data Protection Regulation (GDPR) on time. There is still some space for improvement (e.g., how fast data privacy matters are dealt with by the data protection authority), but it seems that this is not a Poland-specific issue.\(^1\)

Data protection officers and experts are in high demand in both the public and private sectors. Several higher-education bodies offer postgraduate studies focused on privacy and there are GDPR events on a daily basis. The awareness in society regarding privacy is high and probably getting even higher in recent months because of the upcoming GDPR.

New legislation, not necessarily connected to GDPR, was enacted this year or will be enacted soon, including a law to counter terrorism and prevent hate speech on the internet. From many perspectives, and for different reasons, privacy is a topical issue and although there are still aspects that are expected to be regulated in the near future, there are some who may say it is already an overregulated area.

The GDPR will be a game changer not only for businesses, but also for the authorities. Both sides should spend well the few months that are left before 25 May 2018.

II THE YEAR IN REVIEW

This year we have seen a strong focus on preparation of the Polish legal framework for the implementation of the GDPR. The Ministry of Digital Affairs, which is responsible for the introduction of the GDPR into Polish law, published the first draft of the amended Act on the Protection of Personal Data on 23 March 2017. It was widely discussed and after a number of discussions and meetings another draft was published on 14 September. This was followed by a package of drafts of various legal acts where changes were necessitated by the upcoming GDPR. Within the reform package, changes to more than 60 legal acts were proposed, on more than 170 pages of legal text. The changes covered new wording of the E-Commerce Act, the Telecommunications Law, the Act on Insurance Activity, the Act on Payments and the Employment Law. Unfortunately, changes were not proposed for all

---

1 Anna Kobylańska and Marcin Lewoszewski are partners at Kobylańska & Lewoszewski Kancelaria Prawna Sp J.

the legal acts that should, in our view, be reviewed in light of the GDPR. For example, the package does not cover pharmaceutical law (including clinical trials). This, however, will be further discussed with the authorities.

At the same time, the year was full of GDPR-focused meetings with the regulators, legislative bodies, scientists, law practitioners and businesses. Notably, for the first time in Polish history, the International Association of Privacy Professionals held its KnowledgeNet meeting in Poland, attended by more than 120 privacy professionals.

Because of the fast-approaching deadline for the implementation of the NIS Directive on 1 March 2017, the Strategy for Cybersecurity for Poland for 2017–2022 was published by the Ministry of Digital Affairs. The document, consisting of almost 30 pages, describes key strategic directions and plans for the next five years. However, while Deputy Prime Minister Mateusz Morawiecki has confirmed that cybersecurity is one of the authorities’ priorities, and that it should be a Polish export product, there is still no draft law on cybersecurity.

### III REGULATORY FRAMEWORK

#### Privacy and data protection legislation and standards

Privacy law has its roots in the Constitution of the Republic of Poland of 2 April 1997, and in particular in Article 47, which guarantees the right of every citizen to a private life. This constitutional principle was further specified in Articles 23 and 24 of the Act of 13 April 1964 of the Civil Code, which protect the personal interests of natural persons.

Poland implemented EU Directive 95/46/EC by enacting the Act of 29 August 1997 on the Protection of Personal Data (the Act on the Protection of Personal Data). The Act follows the EU Directive and is in compliance with EU law. It is of a general nature and regulates the whole spectrum of processing of personal data by the entities to which the Act applies (including public bodies, associations, individual entrepreneurs and legal entities conducting businesses).

There are secondary regulations to the Act on the Protection of Personal Data that are specific to Poland. For instance, the Ministry of Internal Affairs issued a regulation regarding personal data-processing documentation and technical and organisational conditions that should be fulfilled by devices and computer systems used for personal data processing.

---

7 Journal of Laws 2014, Item 121 with amendments.
processing.\textsuperscript{10} Further, and also specifically Polish, in 2008 the Minister of Internal Affairs and Administration issued a regulation on the specification for a notification of a data filing system for registration with the Inspector General for Personal Data Protection (GIODO).

Data protection is also guaranteed by many sector-specific regulations. There are key legal acts covering data protection in the areas of banking law, insurance law, telecommunications, e-commerce, pharmaceuticals and health law, and other areas where sector-specific provisions regulating how data should be processed are present.

Notwithstanding this regulatory spread, it seems that GIODO has been less active when it comes to enforcement actions and inspections. According to publicly available statistics,\textsuperscript{11} in 2017, GIODO conducted 63 inspections (compared with 192 in 2016) and issued 1,281 administrative decisions (based on inspections and complaints from data subjects). The authority received 1,164 complaints in 2017, compared with 2,610 in previous year.

\section*{ii General obligations for data handlers}

A data controller, when processing personal data, has to ensure:

\begin{itemize}
  \item[a] legal grounds for personal data processing;
  \item[b] limitation of purposes for which personal data are processed;
  \item[c] time limitation of personal data storage;
  \item[d] relevancy and adequacy of the personal data processed by the data controller;
  \item[e] enforcement of data subjects’ rights; and
  \item[f] security of the personal data.
\end{itemize}

Legal grounds for personal data processing include, among others, consent of a data subject, necessity to exercise a contract with the data subject, necessity to exercise rights or duties arising from law, and legitimate interests. The data controllers often ask data subjects to grant their consent but, in fact, all other legal grounds should also be taken into account. Consent of a data subject may be easily withdrawn (at any time after its granting), so it is always worth considering checking out other legal grounds for personal data processing.

The data controller is obliged to inform data subjects about their rights. This information is usually provided by the data controllers upon asking the data subjects’ consent to the processing of their personal data. The information should include: name and address of the data controller, purpose of the data collection, data recipients or categories of data recipient, the existence of the right to access and rectify the data and whether providing the data is voluntary or obligatory. Even more categories of information have to be provided in a situation where the personal data are not collected directly from the data subject.

If the data controller outsources areas of its business, including personal data processing, the data controller is obliged to ensure the outsourced third party (called a data processor) takes proper care of the data. For this reason, the data controller is obliged to enter into a data processing agreement with the data processor. The data processing agreement should include a provision obliging the data processor to process the data solely within the scope of, and for the purpose determined in, the contract.

Moreover, the data controller has to give notice of data filing systems, in which personal data are collected, to the Polish data protection authority. The data controller has to provide the following information about its data filing systems: name and address of the

\begin{itemize}
\end{itemize}
data controller, legal basis for personal data processing, the purpose for the personal data processing, a description of the categories of data subjects and the scope of the processed data, information on the ways and means of data collection and disclosure, information on the recipients or categories of recipients to whom the data may be transferred, a description of the technical and organisational measures applied for the purposes of data security, and information relating to a possible data transfer to a third country. The data filing system notification should take place before the data controller starts processing the personal data. In practice, many data controllers submit the notification after creating a database and collecting personal data therein. There are numerous exemptions from the notification obligation, such as: processing of personal data in connection with an employment relationship; processing of personal data for the purposes of rendering healthcare services, notarial or legal advice, patent agent, tax consultant or auditor services; processing of personal data for the purposes of issuing an invoice or a bill or for accounting purposes; and processing publicly available data. The data controller is also exempted from the notification obligation if he or she has appointed (and registered) a data protection officer. This exemption does not work, however, if the data controller processes sensitive personal data in the data filing system.

The data controller is obliged to secure the personal data against loss or unauthorised access. For this reason the data controller has to apply organisational and technical means appropriate for the type of risk. Polish law requires also, however, that all data controllers apply certain measures that are enlisted in supplementary law provisions, no matter whether they are applicable to a given data controller. As an example, each data controller should apply a similar password policy (e.g., passwords consisting of at least eight characters, changed every 30 days). This solution has been criticised over the years as not meeting the needs of all data controllers.

iii Technological innovation and privacy law

Employee monitoring

As a member of the Article 29 Working Party, GIODO supports the Working Party view regarding employee monitoring. According to public statements by GIODO and its staff, the monitoring of employees is acceptable under Polish law, providing that the employees were informed about the monitoring, the monitoring is not excessive and it does not infringe any of the employees’ personal rights. It seems, therefore, that GIODO follows the judgment of the European Court of Human Rights in the case of Bărbulescu v. Romania.

14 www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF.
Cookies
Polish law on the use of cookies has been introduced as an implementation of EU directives. Storing information on a user's computer, including the use of cookies, is allowed under the following conditions:

a. the user should be informed about the purpose of storing and using the information, and about the possibility of the user configuring the browser or service settings to set rules regarding the use of the information about the user;

b. the user, after receiving this information, consents to this use of his or her data; and

c. the information stored on the user's computer does not cause a change in the settings of the user's computer device or software.

Under Polish law, consent of the user should not be implied. With respect to the consent for the use of information included in cookies, however, the law allows consent to be granted indirectly (by making a choice in a browser's settings). In practice, website users get initial information on the use of cookies each time they open a new website (via a pop-up banner). It is possible to use a website without accepting the cookie policy; however, website owners often require users to click the 'I understand' button before enabling full use of the website.

Non-compliance with the cookie law may result in a financial penalty of up to 3 per cent of the infringer's revenue from the previous year.

Location tracking
In July 2017, GIODO published a broad analysis of the impact of location tracking on privacy. The analysis covers both the Act on the Protection of Personal Data and the GDPR.

According to the authority's stated view, data collected with reference to location tracking should be considered personal data. Therefore, the general rules for processing such data should be applied. The key principles applying to location tracking are the principles of legality, expediency, adequacy, merit correctness, timeliness, and integrity and confidentiality. GIODO considers consent of the individual concerned to be the key legal basis for such processing.

As stated by GIODO within the analysis, just as telecom operators process a particular device's location using base stations, database owners with mapped Wi-Fi access points process personal data when calculating the location of a particular smart mobile device. By specifying both objectives and the means of such processing, these entities become data controllers within the meaning of Article 7(4) of the Act on the Protection of Personal Data (or Article 4(7) of the GDPR).

---

18 Article 23, Section 1(1) of the Act on the Protection of Personal Data.
19 Article 23, Section 1(2) of the Act on the Protection of Personal Data.
20 Article 26, Section 1(3) of the Act on the Protection of Personal Data.
21 Article 26, Section 1(3) of the Act on the Protection of Personal Data.
22 Article 23, Section 1(4) of the Act on the Protection of Personal Data.
23 Article 36 of the Act on the Protection of Personal Data.
Electronic marketing

Following the most recent changes to the Polish law on unsolicited commercial information, the rules of using electronic devices for marketing purposes became unclear. It is forbidden to send commercial information by means of electronic communication (including emails, text messages and internet communicators) without the user’s consent.25 This prohibition is broadly interpreted: even a company logo or a marketing slogan used in an electronic signature may be treated as commercial information. Moreover, this prohibition relates not only to sending emails to private persons, but also to individuals who represent companies. There is also one more prohibition on the use of telecommunication devices or automated calling systems for direct marketing.26 Under this law, companies cannot make phone calls or send emails or text messages with their offers without users’ prior consent. As a result of these two types of prohibition, companies started asking users to grant consent to these two types of action, causing annoyance and lack of understanding on the part of the users.

Spamming may be punished under five different acts of Polish law (the Act on Provision of Services by Electronic Means, the Act on Combating Unfair Competition, the Act on Combating Unfair Market Practices, the Act on Competition and Consumer Protection and the Telecommunications Law) with a maximum financial penalty of up to 10 per cent of the previous year’s turnover. In practice, spammers and cold callers are rarely punished for their actions.

The new rules on the use of electronic devices for marketing purposes are expected with the adoption of the EU ePrivacy Regulation.27

iv Specific regulatory areas

One of most difficult aspects of processing personal data under Polish law relates to the employer–employee relationship. It is common practice for employers to process as much data as possible about employees and candidate employees. However, Polish employment law limits the scope of data than can be processed in such cases. Article 22(1) of the Act of 26 June 1974 on the Labour Code28 provides a list of the data that an employer can request from an employee or candidate employee, including date of birth, education and employment records. Courts have confirmed that employers are not allowed to process data other than those specified in the Labour Code, even with the employee’s consent, because of possible resulting imbalances between the employer and the employee.

The other interesting aspect regarding the processing of candidate employees’ and employees’ data concerns background checks. In practice, the verification of candidates’ past history is limited to the documents they present to the employer and to checking the references supplied (subject to certain conditions). In most parts of the private sector, it would be non-compliant to verify candidates’ criminal records, with an exception for cases such as the employment of bodyguards.

IV INTERNATIONAL DATA TRANSFER

Polish data protection law generally follows EU Directive 95/46/EC when it comes to international data transfers. As a general rule, personal data may be transferred outside the European Economic Area (EEA) if the destination country offers an adequate level of protection for such data. However, if this is not the case, the data controller may rely on one of the following legal bases as grounds for the transfer to the third country:

- the transfer of personal data results from an obligation imposed on the data controller by provisions of law or by provisions of a ratified international agreement that guarantee an adequate level of personal data protection;
- the data subject has given consent in writing for the transfer. Collecting consent is not always possible (e.g., in the case of employees, it should be always verified whether the consent has been freely given);
- the transfer is necessary for the performance of an agreement between the individual concerned and the controller or takes place in response to the relevant individual’s request;
- the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject (e.g., in the case of travel agencies);
- the transfer is necessary for reasons of public interest;
- the transfer is necessary for the establishment of legal claims;
- the transfer is necessary to protect the vital interests of the data subject (e.g., for health reasons);
- the transfer relates to data that are publicly available (e.g., data that constitute an extract from a statutory public register); or
- the transfer takes place upon consent of the data protection authority where the data controller provides adequate data protection safeguards, such as approved model contractual clauses or binding corporate rules.

According to statistics from GIODO, there were only five decisions of the authority in 2017 related to transferring personal data outside the EEA (compared with 11 in 2016). This probably results from the change to the Act on the Protection of Personal Data that led to using EU model clauses (instead of approval by GIODO) as a legal basis for the transfer.

V COMPANY POLICIES AND PRACTICES

Under Polish personal data protection law, each data controller who processes personal data with the use of IT systems is obliged to prepare and implement the following policies:

- a security policy; and
- instructions on managing the IT systems used for personal data processing.

30 Article 36, Section 2 of the Act on the Protection of Personal Data, and Sections 4 and 5 of the Regulation of 29 April 2004 of the Minister of Internal Affairs and Administration as regards personal data processing documentation and the technical and organisational conditions that should be fulfilled by devices and computer systems used for personal data processing.
The scope of these documents is set out in law and includes the following detailed information:

- a list of buildings, premises or their parts comprising the area where the personal data are processed;
- a list of data filing systems with an indication of software used for data processing;
- a description of the structure of the data filing systems and indication of the contents of particular information fields and connections between them;
- the method of transferring data between particular systems;
- a definition of technical and organisational measures necessary to ensure confidentiality, integrity and accountability of the data being processed;
- the procedures for granting authorisation to process data and registration of these authorisations in the computer system as well as an indication of the person responsible for the aforesaid activities;
- the applied methods and means of authorisation and procedures connected with their management and use;
- the procedures for the beginning, suspension and the end of work by the users of the system;
- the procedures for making backups of the data filing systems and programs and software tools used for the data processing;
- the method, place and period of storage of electronic information media containing personal data and backups;
- the method of securing the computer system against malicious software;
- the method of implementation of the requirements to keep records of recipients to whom the data have been disclosed and the dates and the scope of this disclosure; and
- the procedures for executing the inspection and maintenance of systems and information media used for personal data processing.

The requirements as to the type of information that has to be collected by a data controller apply irrespective of its size or the scope of the personal data processed.

VI DISCOVERY AND DISCLOSURE

As a general rule, for the purposes of criminal proceedings, courts and prosecutors may demand any information and documents that may be needed for proceedings, including documents that contain personal data. There are specific provisions of law that relate to revealing personal data for the purposes of criminal proceedings held by authorities from EU countries. Disclosure of personal data to such authorities by Polish institution requires their initial verification as to accuracy and completeness. A disclosing institution may impose certain requirements on data receivers, such as removing or anonymising personal data after a certain time, limiting the scope of personal data processed or refraining from informing data subjects about their personal data processing.

Apart from courts and prosecutors, there are numerous other authorities and institutions that may request a disclosure of information, such as the Polish police force, the Internal Security Agency, the Polish Foreign Intelligence Agency, the Polish Border Guard, the Military Intelligence and Military Counter-Intelligence Services, the Central Anti-Corruption Bureau and the Polish Military Police.

31 Act of 16 September 2011 on Exchanging Information With Investigation Institutions from EU Countries.
VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

According to court judgments, GIODO is the body with authority to supervise and enforce compliance with the law in relation to the processing of personal data.32 Under Article 18 of the Act on the Protection of Personal Data, in the event of any breach of the provisions on personal data protection, the authority, *ex officio* or upon a motion of an individual concerned, by means of an administrative decision, shall order the restoration of the proper legal state, and in particular undertake (1) to remedy the negligence; (2) to complete, update, correct, disclose, or not to disclose personal data; (3) to apply additional measures protecting the collected personal data; (4) to suspend the flow of personal data to a third country; (5) to safeguard the data or to transfer them to other subjects; and (6) to erase the personal data. If the decision issued by GIODO is not followed, the authority may impose a fine of up to €50,000 for a legal person.

In addition, the criminal offences may be prosecuted by the prosecutor, based on Articles 49–54a of the Act on the Protection of Personal Data. According to the statistics published by GIODO on its website, the authority notified the prosecutor of possible criminal offences related to protection of personal data 11 times in 2017, compared with 36 such notifications in 2016.

ii Recent enforcement cases

One of the most discussed decisions issued by GIODO in 2017 is a decision related to the state-owned database of Polish citizens (PESEL). The inspection carried out by GIODO was based on information about probable non-compliant access of bailiffs to the PESEL database for the purpose of the proceedings conducted by the bailiffs in relation to debt collection. GIODO issued a decision against the Ministry of Digital Affairs on 12 September 2017, in which the authority ordered the latter to (1) develop and implement, by 31 December 2017, procedures to be followed in the event of an incident related to the protection of personal data processed under the PESEL register; (2) ensure, before 30 September 2017, that no more than one user can be provided with a certificate card allowing access to the PESEL register by means of tele-transmission; (3) modify, by 31 March 2018, the PESEL access application, so that it can provide a justification for the access to the data processed within the PESEL register; and (4) implement, until 31 December 2017, the software necessary for analysing system logs, including operations performed by users who were granted access to the PESEL registry.

The data protection regulator has also been active in the telecommunications sector. In recent decisions, upheld by the administrative courts, GIODO ordered telecommunications service providers to cease the practice of copying customers’ identification documents. These copies were produced at the point of finalising with customers the agreement for the provision of telecommunications services. The authority, supported by the Office of Electronic Communication, is of the view that this practice is contrary to the Telecommunications Law and the Act on the Protection of Personal Data, as it may result in the processing of data the scope of which is inadequate for the purpose of the agreement.

iii Private litigation

Private litigation in relation to privacy and personal data does not have much of a profile in Poland and case law is scarce in this field. Last year saw very limited proceedings related to infringement of privacy based on civil law and the right to dignity. One of the courts ordered, for example, that installing a CCTV camera in front of a private apartment does not infringe a neighbour’s right to privacy. As stated by the judge deciding the matter: ‘The applicable legal system also grants everyone the personal right to live in their apartment (home), free from disturbances and unrest, and the right to protect their property. These goods are subject to the same protection as the right to privacy.’

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Polish personal data protection law applies to foreign companies if they are located in a third country (a country outside the EEA) but process the personal data with the use of technical means located in Poland.

Companies that act in international groups and have their branch (a local company) located in Poland, should take into account specifics of Polish personal data protection law that may be applicable to their Polish branches, such as:

a a requirement to keep data protection documentation in Polish;

b no option to market the goods or services of another group company on the basis of legitimate interest (only marketing of the branch’s own goods or services is allowed on this basis);

c no option to resign from specific security measures that are required under Polish law (e.g., the requirement to change computer passwords every 30 days);

d strict rules on processing of employees’ personal data (e.g., no option to ask an employee for their criminal record);

e a lack of clear rules on collecting personal data via monitoring (e.g., CCTV monitoring); and

f strict rules on obtaining consent for personal data processing (consent has to be explicit and cannot be a part of a contract or by-laws).

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

While there is no one general act regulating how data should be protected, there are a number of sector-specific regulations covering this issue. In relation to personal data, the key act is the Regulation of 29 April 2004 of the Ministry of Internal Affairs and Administration as regards documentation required to undertake personal data processing, and the technical and organisational conditions that should be fulfilled by devices and computer systems used for personal data processing. The regulation provides some standards for IT systems that process personal data. However, as the regulation is quite old, the standards are outdated and do not guarantee proper levels of security. As the GDPR and the NIS Directive will come into force soon, we anticipate changes regarding how personal data should be protected.

34 Article 3, Section 2 of the Act on the Protection of Personal Data.
This year, the Ministry of Digital Affairs published the Strategy for Cybersecurity for Poland for 2017–2022. The Strategy outlines four goals to be achieved in the given timeframe: (1) achieve capacity for nationally coordinated actions to prevent, detect, combat and minimise the impact of incidents that compromise the security of ICT systems relevant for the functioning of the state; (2) strengthen capacity to address cyberthreats; (3) increase national capacity and competence in cyberspace security; and (4) build a strong international position in cybersecurity.

Crimes that are committed online are regulated by (and prosecuted under) the Polish Criminal Code, which sets out the principles of criminal liability (e.g., in cases of accessing information without the authorisation of the owner). There are also some sector-specific regulations (e.g., for banks, there is ‘Recommendation D on the management of information technology areas and the security of the ICT environment in banks’).

ii Data breaches

There is no general requirement for data controllers (or data processors) to notify a data breach either to the authorities or to data subjects. The only law that requires such notifications is the Telecommunications Law, where the entities providing public telecommunications services are required to notify the Office of Electronic Communications about data breaches. Under Article 174a of the Telecommunications Law, the telecommunications services provider is required to notify the authority about the breach as soon as possible, but not later than 72 hours after the incident. Based on Article 174a, Sections 3 and 4 of the Telecommunications Law, telecommunications services providers are also required to notify affected data subjects about such incidents if they may have a negative impact on individuals’ rights.

There were some significant data breaches this year. For instance, sensitive data of approximately 50,000 patients leaked from one of the public hospitals, and a similar number of records covering employees and contractors leaked from the private postal services provider. Also, the financial sector had its own problems with security. According to a press release, one of the leading providers of loan services was the victim of hackers and as a result suffered a leak of its customers’ data.

X OUTLOOK

Businesses operating in Poland look forward to the final version of the package of legal acts that will implement GDPR. This covers key business sectors, such as banking, insurance, telecommunications and e-commerce. The GDPR will also be a game changer for the regulator itself, as it will face new, sometimes complicated, procedures. We can expect to see some uncertainty in the area of privacy law in the coming years, and from many perspectives.

---

35 See footnote 4.
At the same time, we are still awaiting general regulation of cybersecurity and implementation of the NIS Directive. Data breaches are also becoming more and more difficult to prevent, and the state and businesses should have proper tools to defend against criminal activity.
Data protection and privacy are deemed to be fundamental rights recognised by the Constitution of the Portuguese Republic.

The protection of the privacy of home and correspondence privacy is set forth in Article 34\(^2\) and Article 35\(^3\) of the Constitution, which establish the foundations for the protection of personal data.

Following the EU approach, Portugal has an omnibus data protection legal framework that generally applies to both private and public sectors, as well as to any sector of activity: the Data Protection Act, approved by Law 67/98 of 26 October 1998 (the Data Protection Act).\(^4\),\(^5\)

This legal framework transposes into Portuguese law Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Further to the approval and entering into force of the General Data Protection Regulation (GDPR) on 25 May 2016, Portugal has now begun a process of adjustment to the profound changes that this new law will bring directly upon its application from 25 May 2018 onwards. Until then, the Data Protection Act will continue to apply.

As regards the electronic communications sector, Portugal has approved Law 46/2012 of 29 August (the ePrivacy Act) concerning the processing of personal data and the protection of privacy.\(^6\)
The CNPD, the Portuguese data protection authority – the entity in charge of supervising the application of the regulations on data protection – was created in 1991. It is an independent body with powers within the scope of the Assembly of the Republic, the national parliament.

In recent years, and taking into account the legal and practical evolution of the data privacy framework, data privacy has increasingly become a priority and a concern to market participants in all areas and sectors of activity. However, there are still steps to be taken to ensure that all market participants are duly aware of the possible impact of a data privacy breach – legally, financially and in terms of commercial strategy.

Recent cyberattacks on many Portuguese private companies and public entities have caught the attention of the media, and these, along with the annual national cyberdefence and cybersecurity exercise organised by the Portuguese army, have contributed to creating awareness and know-how on cybersecurity and cyberdefence.

While there is no general cybersecurity or cyberdefence legal framework, there is sectoral legislation concerning the security of communication services and networks.

II THE YEAR IN REVIEW

In the past couple of years, the CNPD has issued several opinions that received wide media attention.

In 2015, the CNPD conducted an audit of the Portuguese Tax and Customs Authority (the Tax Authority) following the creation of a ‘VIP list’ (a list concerning a special group of taxpayers composed of public figures linked to politics and sports). The CNPD concluded that no adequate security measures had been adopted and, therefore, confidentiality was compromised. Also in 2015, the CNPD issued several opinions, including Opinion 1704/2015 on the processing of personal data within clinical investigations; Opinion 1450/2015 on access to data from the electoral registration database; and Opinion 1770/2015 on the intra-group agreements review procedure for transfers of data outside the EU. In 2016, the CNPD issued Opinion 923/2016 on the access of executive officers and solicitors to the personal data included in employees’ payslips in the course of executive processes, and an Opinion on a legislative proposal to provide the Tax Authority with access to bank account data. In July 2017, the CNPD approved Opinion 1039/2017 on the Principles Applicable to the Recording of Phone Calls, revising Opinion 629/2010. In this document, the CNPD defines new time limits for the retention of call recordings for the purpose of proving commercial transactions and any other communications regarding the contractual relationship.

In terms of enforcement actions, in recent years, there has been a clear trend on the part of the CNPD to be more proactive.

In relation to the implementation of the GDPR, the CNPD approved and published a document in January 2017 establishing 10 measures to be taken by entities to prepare for the application of the GDPR. The CNPD has highlighted the main areas of intervention and set out some actions to be taken to ensure compliance with the new legislation. The CNPD will continue issuing guidelines on the GDPR with the purpose of ensuring that it is applied uniformly by the organisations affected. Recently, in August 2017, the government approved Order 163/2017 creating a working group with the purpose of preparing the Portuguese legislation for the application of the GDPR in Portugal.

---

7 To date, this Opinion has not been published.

© 2017 Law Business Research Ltd
As to cybersecurity, in 2015, 2016 and 2017, several attacks on the information systems and websites of public entities were reported, leading to the defacement of websites and disclosure of confidential information. One such attack in 2016 was perpetrated against the information systems of the parliament, the Supreme Court and the police. Following their creation in 2014, the implementation process of the National Cybersecurity Centre and the Cyberdefence Centre continued in 2015 and 2016. In 2015, the National Cyberspace Security Strategy was enacted, setting out the main principles for network and information security, and proclaiming the strategic importance of cybersecurity and cyberdefence in Portugal.

In 2017, the National Cyberspace Security Strategy was approved with the purpose of further developing network and information security, ensuring the defence and protection of critical infrastructure and vital information systems, and enhancing a free, secure and efficient use of cyberspace by all citizens, and by companies and private and public entities.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

In Portugal, the legal data protection framework is regulated by:

a Article 35 of the Constitution;

b the Data Protection Act;

c the ePrivacy Act; and

d Law 32/2008 of 18 July, which sets out the data retention obligations imposed on providers of publicly available electronic communications services.8

There are also data protection provisions in other sector-specific regulations, such as, inter alia, the regulations concerning clinical trials, genetic information and anti-money laundering. The Data Protection Act, applicable until the date on which the GDPR will apply (25 May 2018), aims to protect an individual’s right to private life while processing personal data, establishing the rights and associated procedures of natural persons (data subjects), and the rights, duties and liabilities of legal and natural persons when processing personal data.

‘Personal data’ is defined as information of any type, irrespective of its medium, including sound and image, relating to an identified or identifiable natural person (data subject). Two categories of data set out in the Data Protection Act are classified as sensitive data and require special treatment: (1) data relating to an individual’s philosophical or political beliefs, political party or trade union membership, religion, racial or ethnic origin, health or sex life, including genetic data, and private life data; and (2) data relating to criminal and administrative offences, legal decisions applying penalties or suspected illegal activities.

The controller is the entity directly liable for compliance with the data protection rules. Omission or inadequate compliance with the rules set forth in the Data Protection Act may result in civil or criminal liability or a fine of up to €29,927.88 (up to €5 million under the ePrivacy Act).

Additional penalties may apply, such as data blocking or destruction, temporary or permanent prohibition of processing, or publication of the judgment.

---

8 The validity and enforceability of this Law (as well as corresponding laws in the EU territory) has been uncertain since April 2014 when the Court of Justice of the European Union (CJEU) invalidated Directive 2006/24/EC (which is transposed by this Law) for violating fundamental rights.
General obligations for data handlers

The Data Protection Act sets out principles and obligations that data handlers must comply with when carrying out personal data processing, with controllers and processors having different statuses.

Obligations of data controllers

The controller has a large number of obligations. In particular, the controller shall ensure that:

a. personal data are collected and processed for specified, explicit and legitimate purposes, and their processing is not incompatible with the purposes of the collection;

b. the collected personal data are adequate, relevant and not excessive in relation to the purposes of the collection;

c. personal data are not kept for longer than necessary for the purposes of the collection or processing (and in compliance with CNPD deliberations);

d. adequate technical and organisational measures are adopted to protect and secure the stored personal data;

e. the data subject is provided information concerning the processing, as well as the right of access to rectify his or her personal data; and

f. the CNPD has authorised (usually, for databases containing sensitive data) or has been notified of the processing prior to its commencement.

The data controller must also obtain prior unambiguous consent for the processing of personal data, except when the processing is necessary for certain specific purposes listed in the Data Protection Act.

Controllers must also provide data subjects with information containing:

a. the identity of the controller and of his or her representative, if any;

b. the purposes of the processing;

c. the recipients or categories of recipients;

d. whether replies are mandatory or voluntary, as well as the possible consequences of failure to reply; and

e. the existence and conditions of the rights of access and rectification.

If data are collected through an open network, the data subject must be informed (except when he or she is already aware of the collection) that his or her data may be circulating on the network without security measures, and that the data may be at risk of being seen or used (or a combination of these) by unauthorised third parties.

Obligations of data processors

When the processing is carried out by a processor, the controller must enter into a written agreement with the processor with specific obligations:

a. the processor must act only on the controller’s instructions;

---

9 Personal data processing includes any operation or set of operations performed upon personal data, whether wholly or partly by automatic means, such as the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.
appropriate technical and organisational measures must be implemented by the processor as required by law to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, and all other unlawful forms of processing; and

the data can only be processed on behalf of the controller and solely for the purposes agreed upon.

iii  Technological innovation and privacy law

The CNPD has paid special attention to the challenges of technological innovation, in particular:

a  radio-frequency identification (RFID): the controller must ensure transparent data collection and full data subject information on the use of RFID technology;

b  use of geolocation and monitoring tracking technologies in the employment context: it is indispensable to ensure the right balance between adequate company management and employees’ fundamental rights;

c  automated profiling: online behavioural targeting requires explicit prior subject consent. The CNPD may authorise the processing of data if the processing is adequate and proportional and the data subjects’ rights are not affected;

d  electronic marketing: express prior consent is generally required. The CNPD is particularly attentive to this, since it is one of the most frequent causes for complaints;

e  cookies: as a rule, prior express consent from the data subject is required, and he or she must have received clear and comprehensive information about the underlying purpose;

f  drones: the use of drones poses special privacy concerns. In its Plan of Activities for 2016, the CNPD set the objective to contribute to new regulation on this matter, circumscribing the processing of personal data through those technologies and, whenever the processing takes place, circumscribing the notification exemptions; and

g  internet of things (IoT): in its Plan of Activities for 2016, the CNPD set up a compromise to promote further investigation and education on the IoT’s impact on privacy, considering it one of its priority thematic areas.

iv  Specific regulatory areas

As stated above, the Data Protection Act is the primary legal source on data protection and, therefore, generally applies to any sector and area.

In any case, the privacy issues arising from the specific areas identified below are worth noting.

Employee monitoring

The CNPD published Opinion 7680/2014 setting out the conditions applicable to the processing of personal data regarding the use of geolocation technology in the workplace. In 2016, an interesting judicial decision from the Court of Appeal of Guimarães on the use of a global positioning system in a vehicle within a professional context was issued, ascertaining that the use of such devices to monitor the performance of the worker could be deemed remote surveillance and would not be admitted.
**Electronic marketing**

Under the ePrivacy Act, the delivery of unsolicited communications for direct marketing is subject to prior consent of the subscriber that is an individual or the user. An exception is made for pre-existing relationships: the supplier of a product or service may send advertising regarding its products and services to a client provided that the supplier has the client’s contact details, and only if the advertisement pertains to the same products or services as those the client originally purchased. The client must explicitly be given the opportunity to object to such messaging at the moment of data collection and whenever a message is sent, and there must not be any charges for the recipient in addition to the telecommunication service cost.

**Financial services**

In addition to the Data Protection Act, specific security, bank secrecy and confidentiality obligations apply to financial services organisations. In August 2016, the CNPD issued an Opinion on a legislative proposal to grant the Tax Authority access to bank account data. The proposal provided that Portuguese financial institutions should communicate the value of the deposits of all bank accounts to the Tax Authority. The CNPD considered this proposal illegal, and even unconstitutional. Furthermore, it considered the proposal contrary to the CJEU’s previous decisions on banking secrecy.

IV  INTERNATIONAL DATA TRANSFER

The Data Protection Act distinguishes transfers within the EU from transfers outside the region (to a third country).

Personal data may be freely transferred to another EU Member State, upon notification to the CNPD. In this case, data subjects must be informed if the data are transferred to a third party. For transfers outside the EU, the Data Protection Act distinguishes between countries with an adequate or inadequate level of data protection.

The transfer of personal data to a country that is not a member of the EU may only take place subject to compliance with the Data Protection Act and provided that the receiving country ensures an adequate level of protection.11

The rule is that a transfer of personal data to a country without an adequate level of protection may be allowed by the CNPD if the data subject has unambiguously consented to the proposed transfer (exceptions to this rule apply under the same terms of the 1995 Data Protection Directive).

The CNPD may authorise a transfer or set of transfers to a country that does not ensure an adequate level of protection if the data controller guarantees adequate data protection safeguards. This guarantee can be achieved through appropriate contractual clauses. Authorisation is granted by the CNPD under its own procedures and the decisions of the European Commission (which are typically followed by the CNPD in these matters).

The CNPD issued an opinion in 2004 that clarified the interpretation of Articles 19 and 20 of the Data Protection Act concerning transfers to countries outside the EU. With

---

10 As this Opinion has not yet been published, an identification reference is not available.

11 The adequacy of the level of protection of a country that is not a Member State of the EU is assessed in light of the circumstances surrounding a data transfer or set of transfers. It is for the CNPD or the European Commission to decide whether a country that is not a member of the EU ensures an adequate level of protection.
regard to data transfers to the United States, until the CJEU judgment in *Schrems v. Data Protection Commissioner* on 6 October 2015,\(^{12}\) if a data importer based in the United States was self-certified regarding its adherence to the Safe Harbor Privacy Principles agreed between the EU and the US Department of Commerce, it was considered that the data exporter located in Portugal had the assurance that the company to whom the data were transferred had the adequate level of protection as required by the Data Protection Act.

Following the CJEU *Schrems* decision, the CNPD adopted, on 26 October 2015, a formal decision to issue only temporary authorisations for data transfers to the United States under the various alternatives to the Safe Harbor Privacy Principles, such as standard contractual clauses. Additionally, the CNPD decided to review all authorisations issued since 2000 concerning international data transfers under the Safe Harbor Privacy Principles and, in the meantime, decided that companies should promptly suspend all international data flows to the United States.

More recently, the European Commission adopted the Privacy Shield, a new framework aimed at protecting the personal data of EU citizens that are being transferred to the United States. The CNPD has not yet adopted specific procedures to deal with this new framework. Nonetheless, whenever data are transferred to a data processor, the CNPD considers that the relationship between the data importer and the data exporter (the data controller) must also be ruled by a written agreement.

The European Commission decisions approving standard contractual clauses do not prevent national data protection authorities from authorising other contractual arrangements for the export of data out of the EU based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy. The CNPD recognises the validity of other contractual arrangements for the export of data, provided that the contracts contain specific rules on data protection and comply with the requirements set by the Data Protection Act.

As to binding corporate rules, the CNPD does not accept the transfer of personal data based on unilateral declarations issued by multinational organisations or groups of companies. However, the CNPD has issued the Opinion 1770/2015 on the Intra-Group Agreements, providing that multilateral agreements between companies of the same group would be accepted as long as the data controller declares, in the data transfer notification, that the agreement is in accordance with the model clauses approved by the European Commission. The objective is to expedite the transfer of data outside the EU in these cases.

V COMPANY POLICIES AND PRACTICES

Data controllers may adopt several measures to improve their level of compliance with the data protection rules and reduce the risks associated with breaches of their obligations in this context. The GDPR will bring about a few significant changes to the current policies and practices, including new obligations and requirements. However, and for the time being, the current legislation lists the following measures to be implemented by data controllers.

\(^{12}\) CJEU Case C-362/14 (*Maximilian Schrems v. Data Protection Commissioner*).
i **Compliance programmes**

These programmes generally involve three phases: an audit of all data processing being carried out; definition of the actions required to assure compliance with the data protection law; and the implementation of measures allowing data controllers to have a ‘full picture’ of the relevant data protection matters in the context of their activity, and to provide them with the knowledge needed to manage data protection compliance.

ii **Privacy officers**

The appointment of a person responsible for data protection issues (the data privacy officer) is an important measure to assure compliance with the data protection obligations, notably in large organisations.

iii **Regular audits**

Regular audits are a determining factor for compliance with the Data Protection Act rules. It is fundamental for evaluating whether the purposes that determined the collection and the data storage periods, as well as the remaining data protection obligations, are being respected.

iv **Privacy impact assessments (PIAs)**

Without prejudice to overall continuous efforts to ensure compliance, PIAs should be carried out at the onset of a project with data processing operations. PIAs are an increasingly useful component of a privacy-by-design approach (i.e., where specific privacy features should be installed for specific operations, depending on the purpose and circumstances involved in each specific project). PIAs can reduce the risk of non-compliance, and are helpful in designing efficient processes for handling personal data.

v **Data protection policies**

Companies wishing to implement best practices regarding privacy matters should adopt specific policies and practices so as to comply with the Data Protection Act (e.g., an online privacy and cookies policy, data processing agreements, written consent and informative notices).

vi **Security polices**

Because of a real risk of loss and unauthorised disclosure of personal data, it is essential to adopt security policies with clear rules on the prevention of, and reaction to, a data breach situation.

VI **DISCOVERY AND DISCLOSURE**

The disclosure of personal data in response to national government requests varies significantly depending on the type of data requested.

For instance, disclosure of data collected in the context of the provision of electronic communication services is subject to the constitutional right to the confidentiality of private communications found in Article 34 Paragraph 1 of the Constitution. Furthermore, the Constitution prohibits government interference in private communications, with the only exception consisting in interference for criminal procedure purposes, in accordance with the applicable laws.
The Portuguese Criminal Code provides for the court-ordered interception of private communications in restricted circumstances. This interception can only take place for the purpose of investigating certain crimes.

Additionally, under Law 32/2008 of 18 July, providers of publicly available electronic communications services or of a public communications network must retain certain traffic and location data as well as certain data that allow for the identification of the subscriber or the user of the service. This data must be retained for one year from the date of the communication, and may only be accessed with a court order and for the purpose of the investigation, detection and prosecution of serious crime, as defined by Law 32/2008.

The CNPD Plan of Activities for 2016 sets up the analysis of legislation on data retention in the light of the CJEU decision on the invalidity of EU Directive 2006/24/EC as one of its top priorities.

With regard to foreign government requests, the same limitations apply: disclosure of communication data in response to these requests can only take place for criminal procedure purposes. The disclosure of other types of data is generally subject to the provisions regarding transfers of data to third entities. As expressly provided for in certain contexts, such as cybercrime or digital forensics for criminal investigation purposes (Law 109/2009 of 15 September), national authorities must cooperate with foreign authorities in accordance with the rules on data transfer to third countries.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies
The CNPD is responsible for supervising and monitoring compliance with data protection laws and regulations. Its enforcement powers include the authority to order the blocking, deletion or destruction of data, or the imposition of a temporary or permanent ban on the processing of personal data.

The CNPD actively investigates complaints received from individuals, and the number of inspections is growing significantly.

ii Recent enforcement cases
In line with its Plan of Activities to 2016, the CNPD has turned its attention on the marketing sector, and many recent enforcement actions have been related to direct marketing.

iii Private litigation
Data subjects may claim damages arising from the breach of their data protection rights before the civil courts.

Several decisions resulting from civil claims have focused increasingly on the privacy implications of new technologies, products and services, as well as social media. For instance, it has been deemed appropriate and proportional to impose on parents the duty to refrain from disseminating photos or information that allows the identification of their children on social networks so as to safeguard their right to privacy and the protection of their personal data and security in cyberspace.

In respect of personal data processing in social networks, it has been ruled that information shared through a group of friends on Facebook is considered public information.
from the point of sharing onwards, and valid as evidence within disciplinary proceedings since, from this moment on, the personal data no longer enjoy proper protection under the right to confidentiality in communications.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Data Protection Act is applicable to the processing of personal data where:

a. the processing is carried out in the context of the activities of an establishment of the controller on Portuguese territory;\(^\text{13}\)

b. the controller is not established on Portuguese territory, but in a place where Portuguese law applies by virtue of international public law; or

c. the controller is not established on EU territory and, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on Portuguese territory, unless the equipment is only used for the purposes of transit through the territory of the EU.

Should the Data Protection Act apply to foreign organisations, the major compliance issues arise from international transfers (in particular, the fact that the CNPD does not recognise the validity of binding corporate rules), the information and consent rules, as well as the obligation to obtain the prior authorisation of the CNPD for certain data processing operations.

IX CYBERSECURITY AND DATA BREACHES

There is no general cybersecurity legislation in Portugal. However, there is legislation concerning the security of communication services and networks in the electronic communications sector. Entities providing publicly available electronic communications services in public communications networks must comply with Law 5/2004 of 10 February\(^\text{14}\) (the Electronic Communications Law) and the ePrivacy Law. Under these laws, in the event of a security or integrity breach, these providers should notify the regulator (the National Communications Authority, or ANACOM),\(^\text{15}\) the CNPD and, in some circumstances, service subscribers and users. In addition, more data breach notification obligations will apply in the future, with the application of the GDPR, since this legislation provides for notification to Data Protection Act obligations in all data breaches, independently of the sector in which these breaches occur.

The most important event in the context of cybersecurity in 2016 consisted of the approval of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the EU (the NIS Directive) on 6 July 2016. This Directive will allow the extension to other entities of the obligation to implement security measures and to notify security breaches. Along with the GDPR, the NIS Directive will definitely contribute to more robust information security. Member States must adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with the NIS Directive.

\(^{13}\) The CNPD generally considers that a PO box may be deemed an ‘establishment’ for the purposes of the Data Protection Act.


\(^{15}\) Formerly the Institute of Communications of Portugal, or ICP.
Regarding cybercrime, Portugal is a party to the Council of Europe’s Convention on Cybercrime. Accordingly, the Portuguese criminal system protects confidentiality, integrity, availability and functionality of computer systems and of computer data. Almost all the provisions of the Convention on Cybercrime are transposed into the Portuguese legal system, mainly through the Cybercrime Act. The National Cyberspace Security Strategy, approved by Resolution of the Council of Ministers 36/2015 of 12 June, has set the road map for cybersecurity in Portugal for the next few years, setting up the main intervention axes for the National Cybersecurity Centre.

X OUTLOOK

The CNPD Plan of Activities for 2017 has been guiding its operations during the year, focusing on the evaluation of the Schengen Information System and the Visa Information System and, naturally, on the implementation of the GDPR in Portugal.

The CNPD’s priority is to support the transition to the new legal framework enshrined in the GDPR, given that it will be fully applicable as of May 2018. For that purpose, the CNPD will have to prepare and reinforce its services to ensure the appropriate response to the new challenges arising from the GDPR, while struggling with a significant lack of human resources and funds. The CNPD has also undertaken to study the main changes introduced by the GDPR, contributing to the creation of a new legal framework for the protection of citizens’ fundamental rights.

In January 2017, as indicated above, the CNPD approved and published a document establishing 10 measures to be taken by entities to prepare for the application of the GDPR. The CNPD has highlighted the main areas of intervention and set out some actions to be taken to ensure compliance with the new legislation. The CNPD will continue issuing guidelines on the GDPR with the purpose of ensuring that it is applied uniformly by the organisations affected.

Thus, we expect that active intervention and enforcement actions by the CNPD will increase in the future, with a growing impact on the way data protection is undertaken by data controllers. We believe that the adoption of the GDPR will also have a major impact on the level of awareness regarding data protection matters, and will influence the way data controllers ‘shape’ their compliance strategies.

Notably, in 2015 and 2016, the CNPD published the first issues of its electronic review, Data Protection Forum, which address some of the most recent and relevant topics on privacy and data protection.

On the subject of cybersecurity, the approval of the NIS Directive sets 9 May 2018 as the deadline for the adoption and publication of the new legislation, regulation and administrative provisions necessary to comply with this Directive. In 2016, the government conducted studies on cybersecurity and cyberdefence that will ultimately lead to further legislative developments in these areas.

In August 2017, the National Strategy of Security and Cyberspace was approved with the purpose of further developing network and information security, ensuring the defence and protection of critical infrastructure and vital information systems and enhancing a free, secure and efficient use of cyberspace by all citizens, and by companies and private and public entities.
Taking the above into consideration, given the profound shift in the legal framework that both the GDPR and the NIS Directive represent, it is expected that the immediate future will be very challenging for the government, the public and companies operating in relevant sectors, who must prepare themselves and adapt their procedures to ensure compliance with the new requirements that will be applicable in 2018.
I OVERVIEW

In 2005, Russia ratified the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the 1981 Convention). Russia adopted its Federal Law on Personal Data, which is a primary source of legislation in the sphere of data protection and in many respects is similar to the EU data privacy legislation, in 2006. With the Federal Law on Personal Data having only an 11-year history, Russian data privacy regulation is still quite young.

For a number of years, personal data has been somewhere in the middle distance of Russian regulatory and business attention. Personal data has not been a primary interest of the government, business and media, but just an accompaniment to some larger topics. This situation was compounded by the fines for non-compliance with the personal data rules having always been very insignificant.

The situation greatly changed in 2014, when Russia adopted personal data localisation rules, requiring all operators that collect and process the personal data of Russian citizens to use databases located in Russia. New requirements applying to the personal data of all Russian citizens, irrespective of their legal relations with the personal data operators, immediately received a very negative response from the business community. Although the new rules have not banned the cross-border transfer of personal data, many foreign businesses believe that the requirement for primary data processing via Russian databases is excessive.

The new rules also introduced the option to block non-compliant websites on the Russian territory. The supervising authorities have also become significantly more proactive and have proceeded with numerous audits of major Russian companies and local branches of major multinational companies.

In the middle of 2017, Russia increased the fines for different violations of personal data laws up to 75,000 Russian roubles per violation and introduced different types of punishable offences.

Almost simultaneously with the localisation rules, Russia also adopted a set of counter-terrorism amendments requiring ‘organisers of distribution of information on the internet’ to retain data on internet communications on the Russian territory for six months and to disclose it to the Russian authorities. This further set of even more burdensome counter-terrorism amendments was adopted in 2016 and 2017.

---

1 Elena Kukushkina is a counsel and Georgy Mzhavanadze and Vadim Perevalov are associates at Baker & McKenzie – CIS, Limited.
The new rules have seriously impacted some foreign businesses, especially online services. Now, three years having passed following the adoption of the localisation rules, a lot of major foreign companies operating in Russia have rerouted their data flows to comply with these new requirements. At the same time, some foreign companies are still searching for the most feasible compliance options.

II THE YEAR IN REVIEW

Over the past three years, privacy has become one of the hottest topics in Russia. The recent controversial legislative developments prompted a negative reaction from the business community and caused heated discussion in the mass media.

With effect from 1 September 2015, Russia adopted a law that generally requires all personal data operators that collect and process the personal data of Russian citizens to use databases located in Russia. In accordance with the law, operators, when collecting personal data, must ensure that the databases used to record, systematise, accumulate, store, amend, update and retrieve them are located in Russia. These requirements apply to the personal data of all Russian citizens, irrespective of their legal relations with the personal data operators (including employees, customers or any other individuals).

In addition to that, with effect from February 2015, Russia has enacted the first set of counter-terrorism amendments requiring ‘organisers of distribution of information on the internet’ (i.e., essentially any company operating an online communication service) to retain data on internet communications of Russian users, on users themselves and on certain user activities, to store this information on Russian territory for six months and to disclose it to the Russian authorities upon request. The second set of amendments was adopted in summer 2016. According to these, starting from 20 July 2016, online communication service providers will also be required to provide to the authorities information necessary to decrypt the communications of their users upon request. Furthermore, starting from 1 July 2018, both online communication service providers and telecom service providers may be required to retain and store the contents of communications of internet users for a period of up to six months. Additional obligations are implemented for certain categories of online communication service, namely those that operate various chat and messenger services that enable their users to communicate with each other (effective from 1 January 2018). The counter-terrorism amendments also provide for a number of other obligations.

---

3 A personal data operator is a Russian equivalent for both personal data controllers and data processors.
III REGULATORY FRAMEWORK

Privacy and data protection legislation and standards


The Personal Data Law defines personal data as any data related to a directly or indirectly identified or identifiable individual. Personal data includes but is not limited to:

- a person's first name, middle name and last name;
- the year, month, date and place of his or her birth;
- his or her marital and social status; and
- information about his or her welfare, education, profession and income, etc.

Unlike in the EU, Russian law does not have any guidance for the interpretation of ‘directly or indirectly identifiable individuals’, which can potentially result in a very broad definition of personal data. Previously, Russian authorities used a rather narrow interpretation of personal data, in particular, noting that information constitutes personal data only if they allow unambiguous identification of an individual.

However, this no longer appears to be the case, as Russian authorities have recently changed their approach and currently apply a broader interpretation of personal data. For instance, Russia's data protection authority, Roskomnadzor, initiated several law enforcement actions against telecom companies for sale of user activity data to advertising companies, while the Ministry of Communications (the regulator in the area of personal data) has issued non-binding clarifications on a different subject, in which it concluded that, among other things, personal mobile phone numbers and emails by data subjects constitute personal data.

The Personal Data Law specifically establishes special categories of personal data (sensitive data) and also biometric personal data for special protection.

Special categories of personal data include those that relate to the individual’s race, nationality, political views, religious or philosophical beliefs, health and intimate life.

Biometric personal data is defined as data defining physiological or biological features of a person based on which the person’s identity may be disclosed. It is understood that biometric personal data includes records containing data on distinguishing features of a person, fingerprints and photographic images of a person in any form – printed, digital or other.

The Personal Data Law provides very limited grounds for the processing of special or biometric personal data. The most general of these is the prior written consent of the personal data subject, issued in accordance with the requirements of the Personal Data Law.

6 Article 3 of the Personal Data Law.
7 Resolution of the Supreme Court of the Russian Federation No. APG15-7 as of 24 June 2015.
10 Article 10 of the Personal Data Law.
11 Article 11 of the Personal Data Law.
Unlike EU law, Russia does not have the concepts of ‘data controller’ and ‘data processor’. Instead, the Personal Data Law defines a ‘personal data operator’ as an individual, a state body, municipal body or legal entity that, on its own or in cooperation with other persons, organises or performs (or both) processing of personal data and also determines the goals of that personal data processing, the content of the personal data to be processed and the actions (operations) performed with that personal data.12

In addition, the Personal Data Law makes provision for a third-party processing personal data at the assignment of the personal data operator. In such cases, the operator determines the scope and purposes of the data processing.13 Furthermore, in this case, the third party is also considered a personal data operator, with slightly reduced scope of obligations compared with the instructing operator (i.e., there is no special processor status).

Illegal collection and processing of personal data in Russia may result in civil, administrative and even criminal liability (the latter can be applied in cases of illegal collection or dissemination of information on an individual’s private life).

Civil liability may take the form of compensation for ‘moral harm’, a court order to cease violations, or both.14 As far as moral suffering is concerned, Russian court practice is not very supportive of compensation for moral suffering and the amounts awarded tend to be relatively low.

Violations revealed by Roskomnadzor as the supervising authority generally trigger administrative prescriptions to cure the violations, with or without subsequent audit to check compliance. Failure to cure a violation may also theoretically result in an administrative order to suspend or cease processing of personal data in violation of the law.

Administrative liability for initial non-compliance with the Personal Data Law may take the form of an administrative fine, the maximum amount of which is currently relatively low (approximately US$1,300) per violation.15 If any foreign managers of a company receive an administrative punishment and are also subject to any other administrative fines (for any other administrative violation), they risk being denied Russian visas or entry into the Russian Federation.

ii General obligations for data handlers

According to the Personal Data Law, data processing must be based on legitimate grounds,16 and in most cases personal data should be obtained from the personal data subjects (i.e., individuals) themselves.

From a practical perspective, generally this means that the personal data operator must obtain data processing consent from the data subjects. The consent must always be clear and conscious and should reflect the purposes of the data processing, list the processed personal data and processing operations, as well as information about possible transfers of personal data to third-party operators (including companies of the same group). As a general rule, consent from data subjects may be obtained in any form, including orally, in writing, electronically or by means of implicative conduct.

12 Article 3 of the Personal Data Law.
13 Article 6 of the Personal Data Law.
14 Article 24 of the Personal Data Law.
16 Article 6 of the Personal Data Law.
However, in certain cases an operator is required to obtain a specific written consent for the processing of certain types of personal data or performance of particular types of processing activities. For instance, this requirement applies to the transfer of employee data to any third parties (including affiliated companies) and cross-border transfers of personal data to countries that are not deemed to ensure adequate protection of personal data subjects’ rights (see Section IV). Although a written consent does not necessarily mean a hard-copy document, and may be also obtained in an electronic form signed with an e-signature, the obtaining and maintenance of the latter is quite burdensome and is quite rare in practice. Importantly, quite recently Roskomnadzor has opined that it is not sufficient to have one general data processing consent to cover multiple purposes for data processing. During audits, Roskomnadzor has indicated that such general consents violate Russian law. Instead, according to Roskomnadzor’s recent position, operators should obtain separate consents for each specific processing purpose. This position has already been supported by some courts.17

An operator may also use as grounds for data processing the execution or performance of a contract to which a data subject is a party or beneficiary. However, in this case, the data processing must be either directly prescribed or at least reasonably connected with the aims of the contract (i.e., it should be necessary for its performance).

As noted earlier, according to the new data localisation requirements, when collecting personal data, operators must ensure that the databases used to record, systemise, accumulate, store, amend, update and retrieve the data are located in Russia. The above requirements only apply to operators of personal data collecting personal data. According to the clarifications of Russia’s Ministry of Mass Communications, Mincomsvyaz, collection of personal data is an intentional process of gathering personal data from data subjects directly or through specially engaged third parties.

As another duty of the operators, the Personal Data Law establishes a mandatory requirement for operators to notify Roskomnadzor of their personal data processing activities, which must be submitted to Roskomnadzor before the actual commencement of personal data processing.18 The notification does not imply any authorisation and serves informational purposes only. The law establishes several exemptions from the notification requirements, in accordance with which the operator may not be required to notify Roskomnadzor if the personal data are processed in accordance with Russian labour law; or the personal data are received by an operator in connection with the execution by the operator of a contract to which the personal data subject is a party (with some limitations).19

Data operators should remember that the Personal Data Law provides data subjects with a right to obtain information about their data being processed by a particular operator, the reasons for the processing, the destinations for their transfer and certain other information.20

iii Specific regulatory areas
Russian privacy rules are essentially the same for all personal data operators and similarly apply to different categories of data subjects and personal data. However, different industry laws may set out certain exceptions.

17 Ruling of the Ninth Arbitrazh Appeal Court of 16 August 2016 No. 09APII-30182/2016-AK on Case No. A40-17595/16.
18 Article 22 of the Personal Data Law.
19 Id.
20 Article 14 of the Personal Data Law.
For instance, the Central Bank of Russia is vested with a right to enact binding regulations for the supervised industries.\textsuperscript{21} Furthermore, the Central Bank adopted a regulation requiring banks to report all actual and threatened cybersecurity incidents,\textsuperscript{22} although currently there is no requirement in Russian personal data laws to notify data protection authorities or affected data subjects of any data security breach.

Further, employees’ personal data also receives special treatment. For instance, employers cannot disclose it to a third party (including affiliated companies) without specific written consent, signed with an employee’s ‘wet’ signature, other than where this may be required to avert a threat to the employee’s life or health and in other cases provided for by law (for instance, the consent would normally not be required when personal data is shared with the Russian tax authorities, etc.).\textsuperscript{23} Further, any employee’s personal data should be obtained from the corresponding employee him-or herself. The employer must obtain the employee’s written consent before obtaining the employee’s personal data from a third party, in the event that the personal data can only be obtained from the third party. In addition, as a general rule, employers can obtain and process employees’ sensitive data (e.g., data about political, religious and other convictions, race and ethnicity, etc.) only in cases when this is specifically required by law.\textsuperscript{24}

As well as the above general requirements applicable to data processing in Russia, there is sector-specific regulation of areas such as healthcare, science, transport, communications, energy, banking and other financial market areas, the fuel and energy complex, atomic energy, defence, and the space, mining, metallurgy and chemical industries (see Section IX for more details of regulatory developments regarding critical information infrastructure).

### iv Technological innovation and privacy law

Although Russian personal data laws are in many respects similar to the EU personal data laws, they are much less well adapted to the rapidly changing IT environment and do not provide any specific privacy-related regulation of technologies such as cookies, online tracking, behavioural advertising, cloud computing, the internet of things or big data.

In cases where a technology involves the processing of narrowly interpreted personal data, an operator should carefully follow the law, which may significantly impede a particular process. For example, banks and insurance companies that wish to collect data from additional sources would generally be required to obtain consents to perform ‘profiling’. Furthermore, personal data localisation laws may require companies to use databases located on Russian soil (including for systematisation, combination of data from different sources, modifications and data updates, etc.) even before the information could be transferred to a foreign cloud, which results in serious limitations on the use of foreign cloud technologies.

\textsuperscript{21} Article 4 of the Personal Data Law.
\textsuperscript{22} Regulation on Requirements for Protection of Information in the Payment System of the Bank of Russia, adopted by the Bank of Russia on 24 August 2016, N 552-II.
\textsuperscript{23} Article 88 of the Russian Labour Code.
\textsuperscript{24} Ibid., Article 86.
IV INTERNATIONAL DATA TRANSFER

The rules regulating international transfers of personal data are established by the Personal Data Law. The Law distinguishes two types of countries where personal data are transferred to:

a. countries that provide adequate protection of personal data – these are the Member States of the 1981 Convention. In addition, Roskomnadzor recognises certain other countries as providing adequate protection of personal data. Consent of data subjects to transfer their personal data to these countries is only required if there are no other legitimate grounds for the transfer of personal data to a third party and the consent can be obtained in any verifiable form; and

b. countries that do not provide adequate protection of personal data – these are all other countries (including the United States). The prior written consent of data subjects issued in accordance with the specific statutory requirements set forth in the Law is required for the transfer of personal data to these countries (unless the transfer is solely necessary for the performance of an executed contract to which the data subject is a party).

Data localisation limitations must be always taken into account in the case of an international data transfer.

Although Russia is a member of the Asia-Pacific Economic Cooperation (APEC) process, so far it has not specifically implemented the APEC Cross-Border Privacy Rules. Instead, the Personal Data Law is generally based on the provisions of the 1981 Convention.

V COMPANY POLICIES AND PRACTICES

Russian personal data laws and subordinate regulations expressly or implicitly require personal data operators to implement numerous policies and practices, many of which address data security issues. These various requirements are not codified or otherwise systematised, they change from time to time and allow different compliance approaches; for example, a particular document may address one or several issues, while some other issues may be irrelevant for particular operators and may be avoided.

Some of the commonly required policies and practices include:

a. an online privacy policy (mandatory for operators who collect personal data online);

b. an internal policy on employees’ personal data protection, providing for employees’ rights and responsibilities;

c. a policy on third-party personal data protection;

d. an internal data security policy;

e. the appointment of a chief privacy officer plus a personal data security officer or department, as the case may be;

f. the use of data transfer agreements or clauses that govern disclosure of personal data to any third parties, including affiliates;

25 Article 12 of the Personal Data Law.

26 Currently, pursuant to Roskomnadzor Order No. 274 as of 15 March 2013, amended by Order No. 105 as of 15 June 2017, these other countries are Angola, Argentina, Australia, Benin, Canada, Cape Verde, Chile, Costa Rica, Gabon, Israel, Kazakhstan, Malaysia, Mali, Mexico, Mongolia, Morocco, New Zealand, Peru, Qatar, Singapore, South Africa, South Korea, Tunisia.
g a written information security plan (based on an internally designed model of threats) and documents on its implementation status;

h periodic internal security audits;

i the maintaining of various records, including a list of IT systems used for personal data processing, a list of data subject requests and their statuses, and documents confirming the destruction of personal data.

VI DISCOVERY AND DISCLOSURE

Russian laws and enforcement practices are based on the apparent priority of Russian national security interests and public safety over privacy, and Russian authorities are vested with wide powers to collect or intercept private or personal data. The situation may be rather different when it comes to civil cases or foreign investigations.

In 2016, Russia adopted the new version of its counter-terrorism laws (described above), which imposed surveillance duties on almost any over-the-top internet communication services. It also established the first statutory requirement to provide information necessary to ‘decode’ (essentially decrypt) encrypted electronic user communications to Russian security agencies upon their request.

Unlike in cases involving law enforcement authorities, private organisations are limited in their right to collect and process personal data for their internal investigations, especially in cases of intra-group investigations requiring the transfer of personal data to a foreign affiliate or other third parties, since such transfers require the data subject’s prior consent. However, a data subject can revoke its consent at any time.

Unlike in certain jurisdictions, Russian law does not provide for any general obligation of disclosure in civil cases, although it does vest the courts with a power to request specific disclosure in civil cases at the request of a party to the case. In such cases, the requesting party would need to persuade the court that the requested piece of evidence is relevant for the proceedings and prove that it could not obtain the evidence on its own. Failure to comply with a court disclosure order entails the imposition of court fines, which are relatively low and do not exceed US$1,600 for legal entities and US$100 for individuals.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Roskomnadzor is the primary data protection body in Russia. In particular, Roskomnadzor is authorised to, inter alia:

a impose administrative sanctions for violations of data protection laws;

b initiate inclusion of a website violating personal data requirements in the special register of prohibited information (any access to such websites via Russian providers shall be blocked);

c conduct compliance audits and inspections; and

d file court claims for the protection of the general public.

Other government bodies may be responsible for data protection and privacy issues within the limited scope of their authority. For instance, the State Labour Inspectorate deals with the protection of employees’ personal data, while the Federal Service on Surveillance for Consumer Rights Protection and Human Well-being may take legal action (initiate audits
or file court claims) to protect customers’ personal data. Supervision of the technical requirements of data processing equipment is carried out by the Federal Service for Technical and Export Control and the Federal Security Service of Russia.

Nonetheless, Roskomnadzor is the body with responsibility for general data protection and because of recent trends in Russia it has become very active and the scope of its authority has been growing increasingly wider.

The list of companies subject to scheduled audits by Roskomnadzor is published on its website; however, in addition to planned audits, Roskomnadzor is authorised to conduct unscheduled compliance audits and inspections based on claims from a data subject or information in mass media, or as a result of the systematic monitoring of the internet (an unannounced monitoring of websites’ compliance with the privacy laws).

In addition to the right to impose administrative fines, Roskomnadzor may initiate the blocking of access to a website on the basis of a court ruling, provided that a court act confirms a violation of a Personal Data Law requirement by the website.

Failure to comply with a Roskomnadzor order requiring rectification of a violation may trigger administrative liability in the form of an administrative fine of up to US$300 and potential disqualification of the responsible officers, while failure to perform a court ruling may result in administrative or even criminal liability.

Finally, Roskomnadzor tends to publish the results of actions taken against violations, which attract a lot of mass media attention and which can result in bad publicity for a company.

ii Recent enforcement cases

As personal data compliance has become the issue of the day, Roskomnadzor has been constantly increasing its activities in monitoring compliance with personal data requirements. Thus, in 2015 Roskomnadzor conducted 1,264 personal data audits, while in 2016 the total was 1,406. Roskomnadzor found violations in 664 audits, which amounts to 47 per cent of all audits. The most frequent violations include, inter alia, failure to submit a notification to Roskomnadzor of the operator’s data processing activities, incomplete data transfer agreements and illegal processing of personal data. However, the overall amount of fines imposed by Roskomnadzor for personal data violations in 2016 was only 5.9 million Russian roubles, compared with 10.4 million Russian roubles in 2015.

In 2016 Roskomnadzor audited some of major foreign companies operating in Russia. Perhaps, the most significant and notorious enforcement case was the LinkedIn case. Russian courts established that LinkedIn processed personal data in violation of Russian personal data laws and permitted Roskomnadzor to proceed with blocking access to LinkedIn resources. According to a statement by Roskomnadzor’s press secretary, Roskomnadzor took into account reports of multiple personal data leaks from LinkedIn and decided to send two

---

formal requests to verify LinkedIn’s compliance with Russian personal data laws. Reportedly, LinkedIn failed to provide the requested information to Roskomnadzor and Roskomnadzor proceeded with filing the civil lawsuit to block access to LinkedIn in Russia.

During the proceedings, LinkedIn argued that the social network and the website linkedin.com are operated by a company that is not present in Russia and thus Russian data requirements could not apply to it. The court, however, rejected the lack of jurisdiction argument with reference to Paragraph 1 of Article 15 of the Information Law and Article 1212 of the Civil Code of the Russian Federation (which provides for a choice-of-law rule with respect to consumer contracts) and to the fact that LinkedIn was deliberately targeting the territory of the Russian Federation through the use of the Russian language on the website and the option to use advertising in Russian.32

Also, in the middle of 2017, Roskomnadzor reported that it has reached an agreement with Twitter that the latter will transfer its servers with personal data of Russian nationals into Russia by the middle of 2018. Reportedly, Roskomnadzor and Twitter have been negotiating the issue since 2014.33

### Private litigation

As was noted in Section III, individuals who believe that their right to privacy has been violated may file a court claim and request compensation for ‘moral harm’ or a court order to cease violations, or both.

To date, the majority of such claims relate to cases where a bank transfers personal data of a debtor to a debt collection agency without that data subject’s consent. However, the average amount of compensation for moral harm in these cases does not normally exceed 10,000 Russian roubles, meaning that this type of judicial redress is neither very popular nor very effective for individuals.

### VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Perhaps the most major compliance issue that organisations based or operating outside Russia currently face with regard to the Russian data protection regime is the new data localisation requirement discussed in Section III.

The issue of jurisdiction or the application of the localisation rules to the online data collection is not specifically covered by the law. At the same time, Roskomnadzor and Mincomsvyaz tend to believe that localisation requirements should only apply where a website collecting personal data of Russian citizens specifically targets the territory of Russia.

The most recent non-binding comments with respect to the concept of ‘targeting the territory of the Russian Federation’ were provided by Mincomsvyaz on its website.34 According to Mincomsvyaz, the following criteria, inter alia, can be used to determine whether a website targets Russia: a website or some of its pages are translated into Russian; a website provides the option to make payments in Russian roubles; or an agreement concluded through a website may be performed on the territory of Russia (delivery of goods to Russia, rendering of services or use of purchased digital content in the territory of Russia). When personal data of Russian citizens are deliberately collected online, the Russian localisation laws would apply.

---

32 Resolution of Moscow City Court dated 10 November 2016 No. 33-38783/2016.
34 See minsvyaz.ru/ru/personaldata.
In late 2016, Roskomnadzor issued its own non-binding clarifications on the ‘targeting’ criteria for the purposes of the personal data law. Unlike the commentary issued by Mincomsvyaz, it does not contain any discourse on the Russian language being an international language for certain regions. Instead, Roskomnadzor simply listed the criterion of using the Russian language on a website along with other independent criteria for a website targeting Russia.

Multinational companies with a Russian presence may face some other issues related to the Russian data protection laws. For instance, the transfer of personal data of employees employed at Russian entities to global HR databases requires the obtaining of employees’ specific prior written consent (see Section III). The same relates to the transfer of any employee data to any third party, including companies belonging to the same group. Needless to say, the maintenance of global HR databases must be compliant with the data localisation rules (i.e., primary processing of Russian citizens’ personal data should be done via a Russian database).

The necessity to obtain an employee’s written consent for the transfer of his or her data to a third party may become an issue in the case of the conducting of internal investigations. As a practical solution, it is always recommendable to obtain very full data processing consents at the moment of hiring employees – this would allow proceeding without the necessity to obtain their consent when a conflict situation has emerged.

IX  CYBERSECURITY AND DATA BREACHES

Russia does not participate in any notable international cybersecurity initiatives such as the Council of Europe’s Convention on Cybercrime. Russia also does not have any codified or otherwise systematised cybersecurity requirements, which may differ substantially for various types of confidential information.

Russian laws provide for numerous categories of confidential information, ranging from heavily regulated areas such as state secrets and personal data to almost unregulated types of confidential data, such as secrecy of communications and attorney–client privilege.

To the extent that cybersecurity activities do not concern any of the highly regulated areas, Russian laws are generally silent on cybersecurity issues and do not specifically prohibit or restrict cybersecurity measures such as deep-packet inspections, traffic monitoring or malicious signature monitoring, although in some cases these technologies may raise general privacy issues or issues relating to the secrecy of communications. Nor do Russian laws provide for any general data breach notification obligations, except in relation to specially regulated areas.

In particular, in summer 2017, Russia passed a new law designed to ensure the security of critical information infrastructure facilities in Russia. This law will apply to companies operating information systems in the areas of healthcare, science, transport, communications, energy, banking and other financial market areas, the fuel and energy complex, atomic energy, defence, and the space, mining, metallurgy and chemical industries, as well as to persons that maintain the interaction of such systems. Among other things, the relevant persons will be required to notify Russian authorities of computer incidents, cooperate with officials responsible for tackling computer attacks and observe the conditions for use of protective measures. The law will come into force from 1 January 2018.35

Unlike cybersecurity laws, which have only started to develop and are not very detailed yet, Russian personal data laws and subordinate regulations provide for detailed and very extensive requirements regarding organisational, legal, technical and physical safeguards for personal data.36

The technical measures largely depend on the types of personal data and amount of data subjects whose personal data are processed in a particular information system, while legal and organisational measures are essentially the same and require appointment of data security officers or departments, restrictions of access to personal data and the implementation of various policies and procedures to ensure continuous maintenance of the security of personal data.

Unlike in other jurisdictions, Russia’s data security regulations arguably require the use of locally certified data protection facilities such as antivirus software and firewalls. Such products are available from both Russian and multinational product developers, but must be accompanied with valid certificates from the Federal Service for Technical and Export Control and may differ slightly from their globally available versions (e.g., they may use local update servers in Russia).

The supervisory powers in the relevant area are shared between Roskomnadzor, which is responsible for supervision of the general compliance with personal data laws, the Federal Security Service (if the technical safeguards include cryptographic facilities) and the Federal Service for Technical and Export Control (if cryptographic facilities are not used).

X OUTLOOK

Currently, there are multiple legislative initiatives in Russia concerning privacy and data protection, all of which are at a relatively early stage of development. These include:

a. various potential improvements to the Personal Data Law;

b. regulations on big data; and

c. the potential implementation of the ‘personal information’ concept to regulate data relating to natural persons who cannot be unambiguously identified (e.g., geolocation or behavioural data).

The appearance of more extensive and detailed administrative and court practices, and more detailed clarifications of personal data laws resulting from the much more proactive enforcement approach taken by Roskomnadzor upon the enactment of the personal data localisation requirements, may also be expected.

However, the above changes are unlikely to be as critical as those changes enacted between 2014 and 2016, such as the counter-terrorism laws and personal data localisation requirements, whose effects remain to be seen.

I OVERVIEW

In 2016 and 2017, Singapore continued to rapidly develop its personal data protection, cybercrime and cybersecurity regulatory framework and enforcement initiatives. As set out in Singapore’s October 2016 cybersecurity strategy report, the government views its efforts in these areas as part of an integrated cybersecurity plan to protect the country from cyberthreats and to reinforce Singapore’s standing as a leading information systems hub. The key legal components in this strategy include the Personal Data Protection Act 2012 (PDPA), Singapore’s first comprehensive framework established to ensure the protection of personal data, the Computer Misuse and Cybersecurity Act (CMCA) to combat cybercrime and other cyberthreats, and the upcoming Cybersecurity Act (the Cybersecurity Act), which will be focused on protecting Singapore’s critical information infrastructure (CII) and on establishing a comprehensive national cybersecurity framework.

Although much of the government’s focus in 2017 has been on issuing and passing the proposed Cybersecurity Act, data protection and cybercrime regulation and enforcement both saw significant developments in the past year. With respect to privacy and data protection, the Personal Data Protection Commission (PDPC), the body set up to administer and enforce the PDPA, continued to engage in significant public consultations on aspects of the law and to bring enforcement actions. On cybercrime, the government strengthened existing CMCA provisions and added new cybercrime offences.

In this chapter, we will outline the key aspects of the PDPA, CMCA and the proposed Cybersecurity Act. The chapter will place particular emphasis on the PDPA, including a brief discussion of the key concepts, the obligations imposed on data handlers, and the interplay between technology and the PDPA. Specific regulatory areas such as the protection of minors, financial institutions, employees and electronic marketing will also be considered. International data transfer is particularly pertinent in the increasingly connected world; how Singapore navigates between practical considerations and protection of the data will be briefly examined. We also consider the enforcement of the PDPA in the event of non-compliance.

1 Yuet Ming Tham is a partner at Sidley Austin LLP.
3 The government published the proposed Cybersecurity Act in July 2017, and the public consultation period is scheduled to end on 24 August 2017.
This chapter also will review the amendments to the CMCA and the CMCA’s linkages with the related proposed Cybersecurity Act. The discussion will cover the proposed consolidation of cybersecurity authority within Singapore’s Cyber Security Agency (CSA) and the new position of Commission of Cybersecurity that the Cybersecurity Act would establish.

II THE YEAR IN REVIEW

i PDPA developments

There were a number of significant developments related to the PDPA and the PDPC in the 12 months from September 2016 to August 2017. In October 2016, the government moved the PDPC into the newly formed Info-communications Media Development Authority (IMDA), which itself had emerged from a restructuring of two previous entities: the Infocomm Development Authority of Singapore and the Media Development Authority. Officials noted that the PDPC will continue to operate as an independent personal data protection authority but expected that there would be synergies between the PDPC’s activities and IMDA’s mission to protect consumers in the information, communication and media sectors.

Although there were no new PDPA-related regulations or subsidiary legislation issued in 2016 and the first half of 2017, the PDPC continued to be very active in issuing advisory guidelines. These guidelines are advisory and not legally binding but provide essential guidance for companies seeking to comply with the provisions of the PDPA. The advisory guidelines updates include:

a PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act, issued on 24 September 2013 and revised on 27 July 2017 (the PDPA Key Concepts Guidelines); 4

b PDPC Advisory Guidelines on the Personal Data Protection Act for Selected Topics, issued on 24 September 2013 and revised on 28 March 2017 (the PDPA Selected Topics Guidelines); 5

c PDPC Advisory Guidelines on the Do Not Call Provisions, issued on 26 December 2013 and revised on 27 July 2017 (the PDPA Do Not Call Guidelines); 6

d PDPC Advisory Guidelines on Application of PDPA to Election Activities, issued on 8 July 2017; and

e PDPC Advisory Guidelines for the Healthcare Sector, issued on 11 September 2014 and revised on 28 March 2017 (the PDPA Healthcare Guidelines).

4 The PDPA Key Concepts Guidelines, as with the other advisory guidelines, elaborate on and provide illustrations for the key obligations and interpretation of key terms in the PDPA. The 27 July 2017 revision primarily clarifies the definition of ‘personal data’ in Chapter 5 based on 2016 and 2017 enforcement decisions by the PDPC.

5 The PDPA Selected Topics Guidelines elaborate on how the PDPA applies to certain issues and domains, such as photography and video recordings, employment and research. The 28 March 2017 revision to the PDPA Selected Topics Guidelines updates Chapter 3 to provide additional guidance on using and disclosing anonymised data, including further information on the considerations for assessing and managing the risk of re-identification.

6 The PDPA Do Not Call Guidelines provide examples of how the PDPA Do Not Call (DNC) provisions apply in different situations. The 27 July 2017 revisions to Chapters 3, 7 and 11 provide additional clarifications on dealing with third parties and the definition of an ‘ongoing relationship’.
On 27 July 2017, the PDPC also issued a public consultation notice on important potential changes to PDPA implementation and enforcement. In this Public Consultation for Approaches to Managing Personal Data in the Digital Economy, the PDPC requested public views on two key areas: a proposed ‘enhanced framework’ for collection, use and disclosure of personal data, and a proposed mandatory data breach notification requirement.

These proposals could have significant impacts on Singapore’s data protection regime. With the enhanced framework, the PDPC proposed allowing for collection, use and disclosure of personal data under the PDPA without requiring consent in certain circumstances and only requiring a notification of purpose. These situations may include where an organisation has customer data but no customer contact information or when a company records data in high-traffic areas that may include personal information. In addition, the PDPC proposed establishing a ‘legal or business purpose’ exception to the consent, and in some situations, even the notification requirement. (The PDPA already provides certain exceptions to the consent requirement, such as debt collection or in investigations.) With respect to the data breach proposal, the PDPC noted that there is no requirement that an organisation inform any party when a breach has occurred. The PDPC proposed introducing a mandatory data breach notification to notify any affected individuals. In addition, the PDPC proposed requiring data breach reporting to the PDPC if the number of individuals affected is 500 or more. The consultation period for this notice ends on 21 September 2017.

ii  CMCA developments and the proposed Cybersecurity Act

The CMCA and the proposed Cybersecurity Act are closely linked. In the October 2016 Cybersecurity Report, the government noted the need for a comprehensive framework to prevent and manage the increasingly sophisticated threats to Singapore’s cybersecurity. According to the report, the proposed Cybersecurity Act would establish that framework and would complement the existing cybercrime measures set out in the CMCA.

In 2013, the government amended the existing Computer Misuse Act, renaming it the Computer Misuse and Cybersecurity Act, to strengthen the country’s response to national-level cyberthreats. In 2017, the government introduced further amendments to the CMCA, and the amended law came into effect on 1 June 2017. The amendments broadened the scope of the CMCA by criminalising certain conduct not already covered by the existing law and enhancing penalties in certain situations. For example, the new provisions of the CMCA criminalise the use of stolen data to carry out a crime even if the offender did not steal the data him or herself, and prohibits the use of programs or devices used to facilitate computer crimes, such as malware or code crackers. The amendments also extended the extraterritorial reach of the CMCA by covering actions by persons targeting systems that result in, or create a significant risk of, serious harm in Singapore, even if the persons and systems are both located outside Singapore.

In keeping with the government’s emphasis on safeguarding critical information infrastructure, on 10 July 2017, the Ministry of Communications and Information and the CSA issued the draft Cybersecurity Act for public comment. The proposed Cybersecurity Act focuses on the protection of CII, defined as computer systems necessary for the delivery of certain ‘essential services’, the loss of which would have a severe impact on key sectors such as defence, public health and safety. As defined by the bill, essential services would include energy, telecommunications, healthcare, banking and finance, media and other sectors – 11 in total. The proposed act would impose a number of new obligations on CII owners and would implement a licensing system for cybersecurity service providers. The proposed act
would establish also a new Commissioner of Cybersecurity (a post apparently filled by the current head of the CSA) with wide-ranging supervisory, investigatory and enforcement powers. The public comment period ended on 24 August 2017 and, at the time of writing, the government has not yet issued the final statutory text.

iii 2017 Developments and regulatory compliance

Although the developments with the CMCA and the proposed Cybersecurity Act represent significant milestones in Singapore’s overall cybersecurity strategy, the key compliance framework from the perspective of companies and organisations remains at this point with data protection and privacy. The CMCA is primarily a criminal statute, and the government has not issued any regulations or guidelines for the CMCA. The proposed Cybersecurity Act would impose a number of legal requirements on CII owners and cybersecurity service providers, but the final law has not yet been issued. Once (or if) the Cybersecurity Act comes into effect, the government is likely to need to issue implementing regulations or advisory guidance, or both, to clarify the various obligations on affected organisations. Until that point, organisations’ focus will be on the PDPA and its related regulations, subsidiary legislation and advisory guidelines.\(^7\)

III PDPA REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The PDPA framework is built around the concepts of consent, purpose and reasonableness. The main concept may be summarised as follows: organisations may collect, use or disclose personal data only with the individual's knowledge and consent (subject to certain exceptions) for a purpose that would be considered appropriate to a reasonable person in the circumstances.

There is no prescribed list of ‘personal data’; rather, these are defined broadly as data about an individual, whether or not they are true, who can be identified from that data or in conjunction with other information to which the organisation has or is likely to have access.\(^8\) In addition, the PDPA does not distinguish between personal data in its different forms or mediums. Thus, there is no distinction made for personal data that are ‘sensitive’, or between data that are in electronic or hard copy formats. There are also no ownership rights conferred on personal data to individuals or organisations.\(^9\) There are certain exceptions to which the PDPA would apply. Business contact information of an individual generally falls outside the ambit of the PDPA,\(^10\) as does personal data that is publicly available.\(^11\) In addition, personal data of an individual who has been deceased for over 10 years\(^12\) and personal data contained within records for over 100 years is exempt.\(^13\)

\(^7\) Government agencies are not covered by the scope of the PDPA.
\(^8\) Section 2 of the PDPA.
\(^9\) Section 5.30, PDPA Key Concepts Guidelines.
\(^10\) Section 4(5) of the PDPA.
\(^11\) Second Schedule Paragraph 1(c); Third Schedule Paragraph 1(c); Fourth Schedule Paragraph 1(d) of the PDPA.
\(^12\) Section 4(4)(b) of the PDPA. The protection of personal data of individuals deceased for less than 10 years is limited; only obligations relating to disclosure and protection (Section 24) continue to apply.
\(^13\) Section 4(4) of the PDPA.

© 2017 Law Business Research Ltd
Pursuant to the PDPA, organisations are responsible for personal data in their possession or under their control. ‘Organisations’ include individuals who are resident in Singapore, local and foreign companies, associations and bodies (incorporated and unincorporated), whether or not they have an office or a place of business in Singapore. The PDPA does not apply to public agencies. Individuals acting in a personal or domestic capacity, or where they are an employee acting in the course of employment within an organisation, are similarly excluded from the obligations imposed by the PDPA.

Where an organisation acts in the capacity of a data intermediary, namely an organisation that processes data on another’s behalf, it would only be subject to the protection and retention obligations under the PDPA. The organisation that engaged its services remains fully responsible in respect of the data as if it had processed the data on its own.

There is no requirement to prove harm or injury to establish an offence under the PDPA, although this would be necessary in calculating damages or any other relief to be awarded to the individual in a private civil action against the non-compliant organisation.

Subsidiary legislation to the PDPA includes implementing regulations relating to the DNC Registry, enforcement, composition of offences, requests for access to and correction of personal data, and the transfer of personal data outside Singapore.

There is also various sector-specific legislation, such as the Banking Act, the Telecommunications Act and the Private Hospitals and Medical Clinics Act, imposing specific data protection obligations. All organisations will have to comply with PDPA requirements in addition to the existing sector-specific requirements. In the event of any inconsistencies, the provisions of other laws will prevail.

As mentioned in Section I, to ease organisations into the new data protection regime, the PDPC has released various advisory guidelines, as well as sector-specific advisory guidelines for the telecommunications, real estate agency, education, social services and healthcare sectors. The PDPC has also published advisory guidelines on data protection relating to specific topics such as photography, analytics and research, data activities relating to minors and employment. While the advisory guidelines are not legally binding, they provide helpful insight and guidance into problems particular to each sector or area.

**ii General obligations for data handlers**
The PDPA sets out nine key obligations in relation to how organisations collect, use and disclose personal data, as briefly described below.

---

14 Section 11(2) of the PDPA.
15 Section 2 of the PDPA.
16 Section 4(1)(c) of the PDPA.
17 Section 4(1)(a) and (b) of the PDPA.
18 Section 4(3) of the PDPA.
19 Section 32 of the PDPA.
20 Personal Data Protection (Do Not Call Registry) Regulations 2013.
21 Personal Data Protection (Enforcement) Regulations 2014.
22 Personal Data Protection (Composition of Offences) Regulations 2013.
23 Personal Data Protection Regulations 2014.
24 Section 6 of the PDPA.
Consent\textsuperscript{25}

An organisation may only collect, use or disclose personal data for purposes to which an individual has consented. Where the individual provided the information voluntarily and it was reasonable in the circumstances, the consent may be presumed. Consent may be withdrawn at any time with reasonable notice.\textsuperscript{26} The provision of a service or product must not be made conditional upon the provision of consent beyond what is reasonable to provide that product or service.

An organisation may obtain personal data with the consent of the individual from a third party source under certain circumstances. For example, with organisations that operate in a group structure, it is possible for one organisation in the group to obtain consent to the collection, use and disclosure of an individual’s personal data for the purposes of the other organisations within the corporate group.\textsuperscript{27}

Purpose limitation\textsuperscript{28}

Organisations are limited to collecting, using or disclosing personal data for purposes that a reasonable person would consider appropriate in the circumstances and for a purpose to which the individual has consented.

Notification\textsuperscript{29}

Organisations are obliged to notify individuals of their purposes for the collection, use and disclosure of the personal data on or before the collection, use and disclosure. The PDPC has also released a guide to notification to assist organisations in providing clearer notifications to consumers on the collection, use and disclosure of personal data that includes suggestions on the layout, language and placement of notifications.\textsuperscript{30}

Access and correction\textsuperscript{31}

Save for certain exceptions, an organisation must, upon request, provide the individual with his or her personal data that the organisation has in its possession or control, and how the said personal data has been or may have been used or disclosed by the organisation during the past year. The organisation may charge a reasonable fee in responding to the access request.

The organisation is also obliged to allow an individual to correct an error or omission in his or her personal data upon request, unless the organisation is satisfied that there are reasonable grounds to deny such a request.\textsuperscript{32}

\textsuperscript{25} Sections 13 to 17 of the PDPA.
\textsuperscript{26} In Section 12.42 of the PDPA Key Concepts Guidelines, the PDPA would consider a withdrawal notice of at least 10 business days from the day on which the organisation receives the withdrawal notice to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame under which the withdrawal of consent will take effect.
\textsuperscript{27} Section 12.32, PDPA Key Concepts Guidelines.
\textsuperscript{28} Section 18 of the PDPA.
\textsuperscript{29} Section 20 of the PDPA.
\textsuperscript{30} PDPC Guide to Notification, issued on 11 September 2014.
\textsuperscript{31} Sections 21 and 22 of the PDPA.
\textsuperscript{32} Section 22(6) and Sixth Schedule of the PDPA.
An organisation should respond to an access or correction request within 30 days, beyond which the organisation should inform the individual in writing of the time frame in which it is able to provide a response to the request.\textsuperscript{33}

**Accuracy**\textsuperscript{34}
An organisation is obliged to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation are accurate and complete if they are likely to be used to make a decision that affects an individual or are likely to be disclosed to another organisation.

**Protection**\textsuperscript{35}
An organisation is obliged to implement reasonable and appropriate security safeguards to protect the personal data in its possession or under its control from unauthorised access or similar risks. As a matter of good practice, organisations are advised to design and organise their security arrangements in accordance with the nature and varying levels of sensitivity of the personal data.\textsuperscript{36}

**Retention limitation**\textsuperscript{37}
An organisation may not retain the personal data for longer than is reasonable for the purpose for which they were collected, and for no longer than is necessary in respect of its business or legal purpose. Beyond that retention period, organisations should either delete or anonymise their records.

**Transfer limitation**\textsuperscript{38}
An organisation may not transfer personal data to a country or territory outside Singapore unless it has taken appropriate steps to ensure that the data protection provisions will be complied with, and that the overseas recipient is able to provide a standard of protection that is comparable to the protection under the PDPA (see Section IV).

**Openness**\textsuperscript{39}
An organisation is obliged to implement necessary policies and procedures in compliance with the PDPA, and to ensure that this information is available publicly.

### iii Technological innovation and privacy law
The PDPC considers that an IP address or network identifier, such as an International Mobile Equipment Identity number, may not on its own be considered personal data as it simply identifies a particular networked device. However, where IP addresses are combined with other information such as cookies, individuals may be identified via their IP addresses, which would thus be considered personal data.

\textsuperscript{33} 15.18, PDPA Key Concepts Guidelines.
\textsuperscript{34} Section 23 of the PDPA.
\textsuperscript{35} Section 24 of the PDPA.
\textsuperscript{36} See discussion in Sections 17.1–17.3, PDPC Key Concepts Guidelines.
\textsuperscript{37} Section 25 of the PDPA.
\textsuperscript{38} Section 26 of the PDPA.
\textsuperscript{39} Sections 11 and 12 of the PDPA.
In relation to organisations collecting data points tied to a specific IP address, for example, to determine the number of unique visitors to a website, the PDPC takes the view that if the individual is not identifiable from the data collected, then the information collected would not be considered personal data. If, on the other hand, an organisation tracks a particular IP address and profiles the websites visited for a period such that the individual becomes identifiable, then the organisation would be found to have collected personal data.

Depending on the purpose for the use of cookies, the PDPA would apply only where cookies collect, use or disclose personal data. Thus, in respect of session cookies that only collect and store technical data, consent is not required.40 Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.41 Express consent may not be necessary in all cases; consent may be reflected when an individual has configured his or her browser setting to accept certain cookies but reject others.

If an organisation wishes to use cloud-based solutions that involve the transfer of personal data to another country, consent of the individual may be obtained pursuant to the organisation providing a written summary of the extent to which the transferred personal data will be protected to a standard comparable with the PDPA.42 It is not clear how practicable this would be in practice; a cloud-computing service may adopt multi-tenancy and data commingling architecture to process data for multiple parties. That said, organisations may take various precautions such as opting for cloud providers with the ability to isolate and identify personal data for protection, and ensure they have established platforms with a robust security and governance framework.

As regards social media, one issue arises where personal data are disclosed on social networking platforms and becomes publicly available. As noted earlier, the collection, use and disclosure of publicly available data is exempt from the requirement to obtain consent. If, however, the individual changes his or her privacy settings so that the personal information is no longer publicly available, the PDPC has adopted the position that, as long as the personal data in question were publicly available at the point of collection, the organisation will be able to use and disclose the same without consent.43

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).44 However, the Selected Topics Advisory Guidelines note that a minor of 13 years or older typically has sufficient understanding to provide consent on his or her own behalf. Where a minor is below the age of 13, an organisation should obtain consent from the minor’s parents or legal guardians on the minor’s behalf.45 The Education Guidelines46 provide further guidance on when educational institutions seeking to collect, use or disclose personal data of minors are required to obtain the consent of the parent or legal guardian of the student.

40 Sections 7.5–7.8, PDPA Selected Topics Guidelines.
41 Section 7.11, PDPA Selected Topics Guidelines.
42 Section 9(4)(a) of the Personal Data Protection Regulations 2014.
43 Section 12.61, PDPA Key Concepts Guidelines.
44 Section 8.1, PDPA Selected Topics Guidelines.
45 Section 14(4) of the PDPA. See also discussion at Section 8.9 of the PDPA Selected Topics Guidelines.
46 Sections 2.5–2.8, PDPC Advisory Guidelines on the Education Sector, issued 11 September 2014.
Given the heightened sensitivity surrounding the treatment of minors, the PDPC recommends that organisations ought to take relevant precautions on this issue. Such precautions may include making the terms and conditions easy to understand for minors, placing additional safeguards in respect of personal data of minors and, where feasible, anonymising their personal data before use or disclosure.

**Financial institutions**

A series of notices issued by the Monetary Authority of Singapore (MAS), the country’s central bank and financial regulatory authority, require various financial institutions to, among other things:

a. upon request, provide access as soon as reasonably practicable to personal data in the possession or under the control of the financial institution, which relates to an individual’s factual identification data such as full name or alias, identification number, residential address, telephone number, date of birth and nationality; and

b. correct an error or omission in relation to the categories of personal data set out above upon request by a customer if the financial institution is satisfied that the request is reasonable.

In addition, legislative changes to the Monetary Authority of Singapore Act, aimed at enhancing the effectiveness of the anti-money laundering and the countering of financing of terrorism (AML/CFT) regime of the financial industry in Singapore, came into force on 26 June 2015.

Following the changes, MAS has the power to share information on financial institutions with its foreign counterparts under their home jurisdiction on AML/CFT issues. MAS may also make AML/CFT supervisory enquiries on behalf of its foreign counterparts. Nonetheless, strong safeguards are in place to prevent abuse and ‘fishing expeditions’. In granting requests for information, MAS will only provide assistance for bona fide requests. Any information shared will be proportionate to the specified purpose, and the foreign AML/CFT authority has to undertake not to use the information for any purpose other than the specified purpose, and to maintain the confidentiality of any information obtained.

**Electronic marketing**

The PDPA contains provisions regarding the establishment of a national DNC Registry and obligations for organisations that send certain kinds of marketing messages to Singapore telephone numbers to comply with these provisions. The PDPA Healthcare Guidelines provide further instructions on how the DNC provisions apply to that sector, particularly in relation to the marketing of drugs to patients. In relation to the DNC Registry, the obligations only apply to senders of messages or calls to Singapore numbers, and where the

---

47 MAS Notice SFA13-N01 regulating approved trustees; MAS Notice SFA04-N02 regulating capital markets intermediaries; MAS Notice FAA-N06 regulating financial advisers; MAS Notice 824 regulating finance companies; MAS Notice 3001 regulating holders of money-changers’ licences and remittance licences; MAS Notice PSOA-N02 regulating holders of stored value facilities; MAS Notice 314 regulating life insurers; MAS Notice 1014 regulating merchant banks; and MAS Notice TCA-N03 regulating trust companies.

48 Section 6 of the PDPC Healthcare Guidelines.
sender is in Singapore when the messages or calls are made, or where the recipient accesses them in Singapore. Where there is a failure to comply with the DNC provisions, fines of up to S$10,000 may be imposed for each offence.

**Employees**

The PDPC provides that organisations should inform employees of the purposes of the collection, use and disclosure of their personal data and obtain their consent. Employers are not required to obtain employee consent in certain instances. For instance, the collection of employee’s personal data for the purpose of managing or terminating the employment relationship does not require the employee’s consent, although employers are still required to notify their employees of the purposes for their collection, use and disclosure. Employees of managing or terminating an employment relationship can include using the employee’s bank account details to issue salaries or monitoring how the employee uses company computer network resources. The PDPA does not prescribe the manner in which employees may be notified of the purposes of the use of their personal data; as such, organisations may decide to inform their employees of these purposes via employment contracts, handbooks or notices on the company intranet.

In addition, collection of employee personal data necessary for ‘evaluative purposes’, such as to determine the suitability of an individual for employment, neither requires the potential employee to consent to, nor to be notified of, their collection, use or disclosure. Other legal obligations, such as to protect confidential information of their employees, will nevertheless continue to apply.

Section 25 of the PDPA requires an organisation to cease to retain documents relating to the personal data of an employee once the retention is no longer necessary.

**IV PDPA AND INTERNATIONAL DATA TRANSFER**

An organisation may only transfer personal data outside Singapore subject to requirements prescribed under the PDPA so as to ensure that the transferred personal data is afforded a standard of protection comparable to the PDPA.

An organisation may transfer personal data overseas if:

- it has taken appropriate steps to ensure that it will comply with the data protection provisions while the personal data remains in its possession or control; and
- it has taken appropriate steps to ensure that the recipient is bound by legally enforceable obligations to protect the personal data in accordance with standards comparable to the

---

49 Paragraph 1(o) Second Schedule, Paragraph 1(j) Third Schedule, and Paragraph 1(s) Fourth Schedule of the PDPA.
50 Paragraph 1(f) Second Schedule, Paragraph 1(f) Third Schedule and Paragraph 1(h) Fourth Schedule of the PDPA.
51 Sections 5.14–5.16 of the PDPA Selected Topics Guidelines.
52 Section 26(1) of the PDPA. The conditions for the transfer of personal data overseas are specified within the Personal Data Protection Regulations 2014.

© 2017 Law Business Research Ltd
PDPA. Such legally enforceable obligations would include any applicable laws of the country to which the personal data is transferred, contractual obligations or binding corporate rules for intra-company transfers.

Notwithstanding the above, an organisation is taken to have satisfied the latter requirement if, *inter alia*, the individual consents to the transfer pursuant to the organisation providing a summary in writing of the extent to which the personal data transferred to another country will be protected to a standard comparable to the PDPA; or where the transfer is necessary for the performance of a contract.

In respect of personal data that simply passes through servers in Singapore en route to an overseas destination, the transferring organisation will be deemed to have complied with the transfer limitation obligation.

The Key Concepts Guidelines also provide examples to illustrate situations in which organisations are deemed to have transferred personal data overseas in compliance with their transfer limitation obligation pursuant to Section 26 of the PDPA, regardless of whether the foreign jurisdiction's privacy laws are comparable to the PDPA. An example is when a tour agency needs to share a customer's details (e.g., his or her name and passport number) to make hotel and flight bookings. The tour agency is deemed to have complied with Section 26 since the transfer is necessary for the performance of the contract between the agency and the customer.

An organisation is also deemed to have complied with the transfer limitation obligation if the transfer is necessary for the performance of a contract between a Singaporean company and a foreign business, and the contract is one that a reasonable person would consider to be in the individual's interest.

Other examples given by the Key Concepts Guidelines include the transferring of publicly available personal data, and transferring a patient's medical records to another hospital where the disclosure is necessary to respond to a medical emergency.

The Key Concepts Guidelines also set out the scope of contractual clauses at Section 19.5 for recipients to comply with the required standard of protection in relation to personal data received so that it is comparable to the protection under the PDPA. The Key Concepts Guidelines sets out in a table (reproduced below) the areas of protection a transferring organisation should minimally set out in its contract in two situations: where the recipient is another organisation (except a data intermediary); and where the recipient is a data intermediary (i.e., an organisation that processes the personal data on behalf of the transferring organisation pursuant to a contract).

53 Regulation 9 of the PDP Regulations.
54 Regulation 10 of the PDP Regulations.
55 Regulation 9(3)(a) and 9(4)(a) of the PDP Regulations.
56 Regulation 9(2)(a) of the PDP Regulations.
57 Issued on 23 September 2013 and revised on 8 May 2015.
V    PDPA AND COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary to meet their obligations under the PDPA.58 Organisations must also develop a complaints mechanism,59 and communicate to their staff the policies and practices they have implemented.60 Information on policies and practices, including the complaints mechanism, is to be made available on request.61 Every organisation is also obliged to appoint a data protection officer, who would be responsible for ensuring the organisation's compliance with the PDPA, and to make the data protection officer's business contact information publicly available.62

As a matter of best practice, an organisation should have in place notices and policies that are clear, easily accessible and comprehensible. Some of the policies and processes that an organisation may consider having in place are set out below.

i    Data protection policy

If an organisation intends to collect personal data from individuals, it would be required to notify them of the purposes for the collection, use and disclosure of the personal data and seek consent before collecting the personal data. It should also state whether the personal data will be disclosed to third parties, and if so, who these organisations are. Further, where it is contemplated that the personal data may be transferred overseas, the organisation should disclose this and provide a summary of the extent to which the personal data would receive protection comparable to that under the PDPA, so that it may obtain consent from the individual for the transfer. The data protection policy may also specify how requests to access and correct the personal data may be made. To satisfy the requirement in the PDPA that data protection policies are available on request, the organisation may wish to make its policy available online.

58 Section 12(a) of the PDPA.
59 Section 12(b) of the PDPA.
60 Section 12(c) of the PDPA.
61 Section 12(d) of the PDPA.
62 Section 11(4) of the PDPA.
ii  Cookie policy

If the corporate website requires collection of personal data or uses cookies that require collection of personal data, users ought to be notified of the purpose for the collection, use or disclosure of the personal data, and prompted for their consent in that regard.

iii  Complaints mechanism

The organisation should develop a process to receive and respond to complaints it receives, and this should be made available to the public.

iv  Contracts with data intermediaries

Contracts with data intermediaries should set out clearly the intermediaries’ obligations, and include clauses relating to the retention period of the data and subsequent deletion or destruction, security arrangements, access and correction procedures, and audit rights of the organisation over the data intermediaries. Where a third party is engaged to collect data on an organisation's behalf, the contract should specify that the collection is conducted in compliance with the data protection provisions.

v  Employee data protection policy

Employees should be notified of how their personal data may be collected, used or disclosed. The mode of notification is not prescribed, and the employer may choose to inform the employee of these purposes via employment contracts, handbooks or notices on the company intranet. Consent is not required if the purpose is to manage or terminate the employment relationship; as an example, the company should notify employees that it may monitor network activities, including company emails, in the event of an audit or review.

vi  Retention and security of personal data

Organisations should ensure that there are policies and processes in place to ensure that personal data are not kept longer than is necessary, and that there are adequate security measures in place to safeguard the personal data. An incident-response plan should also be created to ensure prompt responses to security breaches.

VI  PDPA AND DISCOVERY AND DISCLOSURE

The data protection provisions under the PDPA do not affect any rights or obligations under other laws. As such, where the law mandates disclosure of information that may include personal data, another law would prevail to the extent that it is inconsistent with the PDPA. For instance, the Prevention of Corruption Act imposes a legal duty on a person to disclose any information requested by the authorities. Under those circumstances, the legal obligation to disclose information would prevail over the data protection provisions.

The PDPA has carved out specific exceptions in respect of investigations and proceedings. Thus, an organisation may collect data about an individual without his or her consent where the collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data. Further, an organisation may

---

63  Section 4(6) of the PDPA.
64  Second Schedule, Section 1(e) of the PDPA.
use personal data about an individual without the consent of the individual if the use is necessary for any investigation or proceedings.\textsuperscript{65} These exceptions, however, do not extend to internal audits or investigations. Nevertheless, it may be argued that consent from employees is not required as such audits would fall within the purpose of managing or terminating the employment relationship.\textsuperscript{66} Employees may be notified of such potential purposes of use of their personal data in their employee handbooks or contracts, as the case may be.

On an international scale, Singapore is active in providing legal assistance and in the sharing of information, particularly in respect of criminal matters. That said, the PDPC may not share any information with a foreign data protection body unless there is an undertaking in writing that it will comply with its terms in respect of the disclosed data. This obligation is mutual, and the PDPA also authorises the PDPC to enter into a similar undertaking required for a foreign data protection body where required.\textsuperscript{67}

\section*{VII PDPA PUBLIC AND PRIVATE ENFORCEMENT}

\subsection*{Enforcement agencies}

The PDPC is the key agency responsible for administering and enforcing the PDPA. Its role includes, \textit{inter alia}, reviewing complaints from individuals,\textsuperscript{68} carrying out investigations (whether on its own accord or upon a complaint), and prosecuting and adjudicating on certain matters arising out of the PDPA.\textsuperscript{69}

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,\textsuperscript{70} including the power to require organisations to produce documents or information, and the power to enter premises with or without a warrant to carry out a search. In certain circumstances, the PDPC may obtain a search and seizure order from the state courts to search premises and take possession of any material that appears to be relevant to an investigation.

Where the PDPC is satisfied that there is non-compliance with the data protection provisions, it may issue directions to the infringing organisation to rectify the breach and impose financial penalties up to S$1 million.\textsuperscript{71} The PDPC may also in its discretion compound the offence.\textsuperscript{72} Certain breaches can attract penalties of up to three years’ imprisonment.\textsuperscript{73} In addition to corporate liability, the PDPA may also hold an officer of the company to be individually accountable if the offence was committed with his or her consent or connivance,

\begin{flushright}
\textsuperscript{65} Third Schedule, Section 1(e) of the PDPA.
\textsuperscript{66} As discussed earlier, consent is not required if the purpose for the collection, use and disclosure of personal data is for managing or terminating the employment relationship.
\textsuperscript{67} Section 10(4) of the PDPA.
\textsuperscript{68} Section 28 of the PDPA.
\textsuperscript{69} See Sections 28(2) and 29(1) of the PDPA. The PDPC has the power to give directions in relation to review applications made by complainants and contraventions to Parts III to VI of the PDPA.
\textsuperscript{70} Section 50 of the PDPA. See also Ninth Schedule of the PDPA.
\textsuperscript{71} Section 29 of the PDPA.
\textsuperscript{72} Section 55 of the PDPA.
\textsuperscript{73} Section 56 of the PDPA.
\end{flushright}
or is attributable to his or her neglect. Further, employers are deemed to be vicariously liable for the acts of their employees, unless there is evidence showing that the employer had taken steps to prevent the employee from engaging in the infringing acts.

Directions issued by the PDPC may be appealed to be heard before the Appeal Committee. Thereafter, any appeals against decisions of the Appeal Committee shall lie to the High Court, but only on a point of law or the quantum of the financial penalty. There would be a further right of appeal from the High Court’s decisions to the Court of Appeal, as in the case of the exercise of its original civil jurisdiction.

In relation to breaches of the DNC Registry provisions, an organisation may be liable for fines of up to S$10,000 for each breach.

ii Recent enforcement cases

Starting with the first round of decisions and penalties in April 2016, the PDPC has been active in enforcing violations of the PDPA and has published the grounds of all its decisions on its website and in the first Personal Data Protection Digest, which was released by the PDPC in early 2017. In 2016, the PDPC published 22 decisions, in the majority of which it found the respondents had breached the PDPA. In 2017, the number of published decisions stood at 12 by July 2017. In the decisions, the PDPC provides substantial factual detail and legal reasoning, and the decisions are another source of information for companies seeking guidance on particular issues.

Several enforcement actions in the first half of 2017 set out the PDPC’s typical mix of behaviour remedies combined with financial penalties, including:

a) Propnex Realty Pte Ltd: the PDPC imposed a financial penalty of $10,000 on the respondent for failing to make reasonable security arrangements to prevent unauthorised access of individuals’ personal data stored online. The PDPC also directed the respondent to cease the storage of documents containing personal data until a security scan had been completed.

b) Singapore Telecommunications Ltd and Tech Mahindra Pte Ltd: the PDPC imposed a financial penalty of $10,000 on respondent Tech Mahindra, a data intermediary, for failing to make reasonable security arrangements to prevent unauthorised access and modification of SingTel customers’ personal data via SingTel webpages. The PDPC found no violation for respondent SingTel.

c) National University of Singapore: for the respondent’s failure to prevent the disclosure of student personal data, the PDPC directed the respondent to design training to address data protection related to student events and implement the training for student leaders in charge of organising such events.

d) Orchard Turn Developments Pte Ltd: the PDPC imposed a financial penalty of $15,000 on the respondent for failing to make reasonable security arrangements

---

74 Section 52 of the PDPA.
75 Section 53 of the PDPA.
76 Section 35 of the PDPA.
77 Decision Citation: [2017] SGPDPC 1.
78 Decision Citation: [2017] SGPDPC 4.
79 Decision Citation: [2017] SGPDPC 5.
80 Decision Citation: [2017] SGPDPC 12.
to protect member personal data stored on its server. The PDPC also directed the respondent to patch all vulnerabilities, conduct a penetration test, implement a password management policy and conduct staff training.

iii Private litigation

Anyone who has suffered loss or damage directly arising from a contravention of the data protection provisions may obtain an injunction, declaration, damages or any other relief against the errant organisation in civil proceedings in court. However, if the PDPC has made a decision in respect of a contravention of the PDPA, no private action against the organisation may be taken until after the right of appeal has been exhausted and the final decision is made.81 Once the final decision is made, a person who suffers loss or damage as a result of a contravention of the PDPA may commence civil proceedings directly.82

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to foreign organisations in respect of activities relating to the collection, use and disclosure of personal data in Singapore regardless of their physical presence in Singapore.

Thus, where foreign organisations transfer personal data into Singapore, the data protection provisions would apply in respect of activities involving personal data in Singapore. These obligations imposed under the PDPA may be in addition to any applicable laws in respect of the data activities involving personal data transferred overseas.

IX CYBERSECURITY AND DATA BREACHES

i Data breaches

While the PDPA obliges organisations to protect personal data, there is currently no requirement to notify authorities in the event of a data breach. However, as noted above, in the PDPC’s public consultation of July through September 2017, the PDPC proposed incorporating a requirement that organisations inform affected individuals in the event of a breach and report the incident to the PDPC if there are 500 or more persons affected. In the absence of mandatory data breach requirements, government sector regulators have imposed certain industry-specific reporting obligations. For example, MAS issued a set of notices to financial institutions on 1 July 2014 to direct that all security breaches should be reported to MAS within one hour of discovery.

The proposed Cybersecurity Act represents a move away from sector-based regulation. The Act would require mandatory reporting to the new Commissioner of Cybersecurity of ‘any cybersecurity incident’ (which is broader than but presumably would also include data breaches) that relates to CII or systems connected with CII. In issuing the bill, the government noted that it had considered sector-based cybersecurity legislation but had concluded that an omnibus law that would establish a common and consistent national framework was the better option.

81 Section 32 of the PDPA.

© 2017 Law Business Research Ltd
ii Cybersecurity

Singapore is not a signatory to the Council of Europe’s Convention on Cybercrime.

In Singapore, the CMCA is the key legislation governing cybercrime and cybersecurity, pending the passage of the proposed Cybersecurity Act. The CMCA is primarily focused on defining various cybercrime offences, including criminalising the unauthorised accessing\(^{83}\) or modification of computer material,\(^{84}\) use or interception of a computer service,\(^{85}\) obstruction of use of a computer,\(^{86}\) and unauthorised disclosure of access codes.\(^{87}\) The 2017 amendments to the CMCA added the offences of obtaining or making available personal information that the offender believes was obtained through a computer crime\(^{88}\) and using or supplying software or other items to commit or facilitate the commission of a computer crime.\(^{89}\)

Although the CMCA is in general a criminal statute, the 2013 amendments added a cybersecurity provision in the event of certain critical cybersecurity threats. In particular, the Minister of Home Affairs may direct entities to take such pre-emptive measures as necessary to prevent, detect or counter any cybersecurity threat posed to national security, essential services or the defence of Singapore or foreign relations of Singapore.\(^{90}\) As previously noted, the proposed Cybersecurity Act would greatly expand national cybersecurity protections, including a nearly identical provision granting similarly sweeping powers to the Minister of Media and Communications in the event of a cybersecurity ‘emergency’. More generally, the proposed Cybersecurity Act would mark a new phase in Singapore cybersecurity’s regime by imposing affirmative reporting, auditing and other obligations on CII owners and by appointing a new Commissioner of Cybersecurity with broad authority, including the power to establish mandatory codes of practice and standards of performance for CII owners.

X OUTLOOK

In keeping with its declared strategy, Singapore continues to progress on clarifying and enforcing its existing data privacy and cybersecurity laws and establishing a more robust cybersecurity framework. With the iminent passage of the proposed Cybersecurity Act, 2017 is likely to be viewed as a watershed year in the country’s cybersecurity regulatory regime.

Moving forward, we expect to see a high degree of activity within the government, as well as in the context of public consultations, after the passage of the proposed Cybersecurity Act. As with the PDPA, the government is likely to have to provide substantial guidance, in the form of implementing regulations, subsidiary legislation or advisory guidelines, or both, to clarify vague provisions in the final law and to set out specific administrative mechanisms.

\(^{83}\) Sections 3 and 4 of the CMCA.
\(^{84}\) Section 5 of the CMCA.
\(^{85}\) Section 6 of the CMCA.
\(^{86}\) Section 7 of the CMCA.
\(^{87}\) Section 8 of the CMCA.
\(^{88}\) Section 8A of the CMCA.
\(^{89}\) Section 8B of the CMCA.
\(^{90}\) Section 15A of the CMCA. Essential services include the energy, finance and banking, ICT, security and emergency services, transportation, water, government and healthcare sectors.
We also expect PDPA-related activities to continue. The PDPC currently is considering revisions to the data privacy framework, including implementing a mandatory breach notification requirement. In addition, we expect the PDPC to continue providing guidance on various aspects of the PDPA and to maintain its enforcement vigilance.
I OVERVIEW

Data protection and privacy are distinct rights under Spanish law, but both are deemed fundamental rights derived from respect for the dignity of human beings. They are primarily based on the free choice of individuals to decide whether to share with others (public authorities included) information that relates to them (personal data) or that belongs to their private and family life, home and communications (privacy). Both fundamental rights are recognised in the Lisbon Treaty (the Charter of Fundamental Rights of the European Union) and the Spanish Constitution of 1978. Data protection rules address, *inter alia*, security principles and concrete measures that are helpful to address some cybersecurity issues, in particular, because specific cybersecurity legislation (which not only covers personal data and private information but rather any information) is new and not sufficiently developed yet.

Spain has an omnibus data protection framework law along the lines of the EU approach, and applies it both to the private and public sectors. However, some personal data or some processing activities may require specific protection such as certain financial, e-communications or health-related data or processing activities. There are several codes of conduct for data protection that have been approved in different sectors but, in general terms, they merely adjust the general obligations to the specific needs of the relevant sector or organisation.

The rights to data protection and privacy are not absolute and, where applicable, must be balanced with other fundamental rights or freedoms (e.g., freedom of information or expression) as well as other legitimate interests (e.g., intellectual property rights, public security and prosecution of crimes).

In the case of data protection, this balance must be assessed by the organisation and could be challenged before the Spanish Data Protection Authority (DPA), which is in charge of supervising the application of the regulations on data protection (see Section III.i). Privacy infringements must be claimed before the (civil or criminal) courts.

The DPA was created in 1993, and has been particularly active in its role of educating organisations and the general public on the value of data protection and of imposing significant sanctions. In 2016 alone, the DPA received 10,523 claims from individuals and authorities, and issued and published 654 sanctioning resolutions. These sanctions are published on its website, which is used by the media, among others, as an important source of data protection information.

---

Leticia López-Lapuente and Reyes Bermejo Bosch are lawyers at Uría Menéndez Abogados, SLP.
II  THE YEAR IN REVIEW

The publication of the first draft of the new Data Protection Law implementing Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR) has been the most relevant milestone on data protection in recent months. The draft is nevertheless expected to change and will not receive final approval before May 2018 at the earliest. Regarding the implementation of the Security of Network and Information Systems Directive (the NIS Directive), the Spanish government has just announced that a draft royal decree is being prepared, although its content is not yet publicly available (see Section IX).

Finally, as a consequence of the Google Spain v. Costeja (Google Spain) case in 2014 before the Court of Justice of the European Union (CJEU) (regarding the ‘right to be forgotten’), the DPA has continued to initiate certain proceedings on this matter; several judicial rulings of relevance on a national level (mainly from the Spanish Supreme Court) have been issued in Spain modulating the concept of ‘establishment’ and the rules regarding jurisdiction and applicable law set out by the CJEU in Google Spain (see Section VII.ii).

III  REGULATORY FRAMEWORK

i  Privacy and data protection legislation and standards

The legal framework for the protection of personal data in Spain is regulated by the Lisbon Treaty; Article 18(4) of the Spanish Constitution; and Law 15/1999 of 13 December on the Protection of Personal Data (the DP Law), as developed by Royal Decree 1720/2007 of 21 December (RD 1720/2007) (together, the DP Regulations). As a consequence of the GDPR’s approval, the DP Regulations are currently subject to review. The first draft of the new DP Law was published in July 2017; however, the regulatory process remains at a very preliminary stage. Its final approval would ideally occur in May 2018, although the director of the DPA has recently acknowledged that the deadline is tight.

Sector-specific regulations may also contain data protection provisions, such as the E-Commerce Law 34/2002 (LISS), the General Telecommunications Law 9/2014 (GTL), anti-money laundering legislation and the regulations on biomedical research.

Privacy rights are mainly regulated by Law 1/1982 of 5 May on civil protection of the rights to honour, personal and family privacy, and an individual’s own image, and by the Spanish Criminal Code.

Personal data and private data are not synonymous. Personal data are any kind of information (alphanumeric, graphic, photographic, acoustic, etc.) concerning an identified or identifiable natural person, irrespective of whether or not this information is private. However, data regarding ideology, trade union membership, religion, beliefs, racial origin, health or sex life as well as criminal and administrative offences are deemed more sensitive and require specific protection.

Protecting personal data is achieved by allocating specific duties to both ‘controllers’ (i.e., those who decide on the data processing purposes and means) and ‘processors’ (i.e., those who process the data only on behalf of a controller to render a service).

The DPA is the entity in charge of supervising compliance with the data protection duties imposed by the DP Regulations (fair information, legitimate ground, security,
notification, proportionality and quality, etc.). The DPA has carried out ex officio audits of specific sectors (including online recruitment procedures, TV games and contests, hotels, department stores, distance banking, hospitals, schools, webcams and mobile apps). However, the DPA’s activity in terms of individual compliance investigations has significantly increased over the past 10 years, as has the number of fines imposed. Indeed, failure to comply with the DP Regulations may result in the imposition of administrative fines ranging from €900 to €600,000 per infringement depending on the gravity of the offence (and regardless of whether civil or criminal offences are also committed, if applicable). Neither harm nor injury is required (i.e., the infringement itself suffices for the offender to be deemed liable), but the lack of any harm or injury is considered an attenuating circumstance to grade the amount of the administrative fine. However, harm or injury will be required to claim damages arising from breaches of data protection rights before civil and criminal courts.

ii General obligations for data handlers

Data controllers (irrespective of whether or not they handle the personal data) and data processors must comply with specific obligations set out in the DP Regulations.

Obligations of data controllers

a Any personal data file should be registered (as well as any modifications to it) with the DPA;

b data subjects from whom personal data are requested must be provided beforehand with information about the processing of their personal data;

c as a general rule, controllers must obtain the prior consent of the data subject to any processing activity – including (intra-group) transfers. Furthermore, explicit consent is required for certain processing activities involving ‘sensitive’ data (such as health-related data) or consisting of direct marketing;

d there are few exemptions to the need to obtain the data subject’s prior consent, such as when the processing of the personal data is unavoidable to perform a contract that the data subject has executed with the data controller; or when the data controller engages a third-party services provider that, to perform its services, needs to access or otherwise process personal data held by the data controller, in which case a written agreement with a minimum legally prescribed content (a processing agreement) must be executed. The legitimate interest of the controller or a third party is not expressly recognised by the DP Law as a legitimate ground for the processing of personal data but, according to the judgment in Case C-468/2010, the CJEU has set out the direct applicability in Spain of Article 7(j) of EU Directive 95/46/EC, allowing the processing of that data subject’s personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed;

e when the recipient is not located in the EU or EEA (or in a country whose regulations afford an equivalent or adequate level of protection identified by the European Commission or the DPA), the prior authorisation of the DPA must be obtained, unless a legal exemption applies;

2 The data protection right is enforced by the DPA at a national level with limited exceptions. For example, Catalonia and the Basque Country are regions that have regional data protection authorities with competence limited to the processing of personal data by the regional public sector.
controllers should adopt specific security measures; and
data subjects have a right to access all data relating to them, and to rectify and cancel
data the processing of which does not comply with the data protection principles, in particular, when data are incomplete or inaccurate or excessive in relation to the legitimate purpose of its processing. Data subjects are also entitled to object to certain processing activities that do not require their consent or are made for direct marketing purposes.

Obligations of data processors

Data processors must:

- execute the above-mentioned processing agreement with the relevant data controller;
- implement the above-mentioned security measures;
- process data only to provide the agreed services to the controller and in accordance with its instructions;
- keep the data confidential and not disclose it to third parties (subcontracting is not prohibited but is subject to specific restrictions), even for storage; and
- upon termination of the services, return or destroy the data, at the controller’s discretion.

The GDPR has added certain mandatory content for a processing agreement to be valid (see Article 28.3 of the GDPR). Although the duties of the GDPR will not become mandatory until May 2018, the DPA has publicly encouraged data controllers subject to Spanish law to start implementing the GDPR rules regarding processing agreements before 2018.

iii Specific regulatory areas

The DP Regulations apply to any personal data, but they provide for reinforced protection of data related to children (the verifiable consent of the minor’s parents is required) and health-related data (express consent and specific security measures are required as a general rule). Specific rules also apply to the information processed by solvency and credit files, and to the processing of data for video surveillance or access control purposes.

In addition, certain information is also protected by sector-specific regulations. This is the case for, inter alia:

- financial information that is subject to banking secrecy rules (Law 10/2014 of 26 June 2014 on the regulation, supervision and solvency of credit institutions);
- the use (for purposes other than billing) and retention of traffic and location data (GTL);
- the sources of information and intra-group disclosures to comply with regulations concerning anti-money laundering and combating the financing of terrorism, and restrictions on the transparency principle in relation to data subjects (Law 10/2010 of 28 April on the prevention of money-laundering and financing of terrorism);
- the use of genetic data or information contained in biological samples (Law 14/2007 of 3 July on biomedical research);
- information used for direct-marketing purposes (LISS);
the outsourcing of core financial services to third parties (Royal Decree 84/2015 of 13 February developing Law 10/2014, and Bank of Spain Circular 2/2016 on the supervision and solvency of credit institutions, which adapts the Spanish legal regime to EU Directive 2013/36/EU and EU Regulation 575/2012); and

the use of video-surveillance cameras in public places (Law 4/1997 of 4 August governing the use of video recording in public places by state security forces).

iv Technological innovation

Technology has created specific issues in the privacy field, including:

a Online tracking and behavioural advertising: as a general rule, explicit prior consent is required. The DPA has permitted the application of a legitimate-interest justification to (offline) advertising activities – as provided in the GDPR; however, the DPA does not consider that online behavioural advertising or profiling activities can be based on the existence of a legitimate interest.

b Location tracking: in the past few months, the DPA has issued several resolutions and opinions regarding the use of geolocation tools. In those resolutions, the DPA considers that the use of this technology in work environments may be reasonable and proportionate, but only subject to certain circumstances (mainly, that specific information has been provided to data subjects on its use and purposes).

c Use of cookies: as a general rule, explicit prior consent is required for installing cookies or similar devices on terminal equipment. In 2017, the DPA initiated 62 investigations and issued nine sanctioning resolutions regarding cookies (there are numerous resolutions issuing warnings but not imposing economic sanctions).

d Biometrics: traditionally, the processing of biometric data has not been considered ‘sensitive’ and, therefore, the DPA has made no specific requirements in this area. The implementation of the GDPR in Spain implies a change in the concept of biometrics and we are currently awaiting the DPA’s guidelines in this regard.

e Big-data analytics: in April 2017, the DPA published guidelines on big-data projects. The guidelines were drafted on the basis of the GDPR’s requirements.

f Anonymisation, de-identification and pseudonymisation: the DPA has been working on adopting an official position regarding the use of ‘anonymous’ data and open data in big-data projects. As a result, the DPA published guidelines at the end of 2016 on the protection of personal data related to the reuse of public-sector information and guidelines on anonymisation techniques.

g Internet of things and artificial intelligence: the DPA has not adopted an official position regarding the internet of things and artificial intelligence.

h Data portability: the DPA recently published a legal report on, among other issues, the data portability right. The DPA admits that the portability right includes not only data subjects’ current data, but also their former data (either provided by them or inferred from the contractual relationship); however, the information obtained from the application of profiling techniques (e.g., algorithms) would not be subject to portability. Although the DPA’s legal reports are not binding, they are highly useful since they reflect the DPA’s doctrinal tendency.

i Right of erasure or right to be forgotten: the right to be forgotten in relation to search engines is actively pursued both by Spanish data subjects and the DPA. Notably, Google
Spain, in which the CJEU’s ruling recognised the right to be forgotten, was initiated in Spain and the Spanish DPA had a significant role in the case. There are several DPA resolutions issued every year recognising the right of Spanish individuals to be forgotten and also setting out certain exceptions to the applicability of the right.

Data-ownership issues: to date, there is no Spanish legislation that specifically regulates the question of ownership of data. Notwithstanding this, several regulations exist that may have an impact on data ownership including, among others, data protection legislation, copyright law (which regulates rights over databases) or even unfair competition rules.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

According to the DP Regulations, data transfers from Spain to (or access by) recipients located outside the EEA require the prior authorisation of the DPA, unless the recipient ensures an ‘adequate’ level of protection as recognised by the European Commission (or the DPA) or the transfer can be based on a statutory exemption. The draft of the new DP Law does not include the DPA’s authorisation as a mandatory requirement (the new DP Law would be aligned with the GDPR).

Irrespective of the authorisation requirement, all international data transfers outside the EEA must be notified to the DPA for registration.

The authorisation of the DPA will be granted if the data exporter (controller or processor) provides adequate safeguards, such as by executing the European Commission’s standard contractual clauses for data transfers or other clauses such as the standard contractual processor-to-processor clauses, approved by the DPA in 2012 to enable the subcontracting of non-EEA subcontractors by service providers established in Spain. In Spain, data transfer agreements must be previously authorised by the DPA, even if they are based on any of these clauses.

Spanish law also allows the DPA to grant authorisation based on binding corporate rules (BCRs) adopted within a group. Spain is a mutual recognition procedure (MRP) country; thus, the BCRs approved by the leading data protection authority of any MRP country must be recognised in Spain. The granting of the authorisation entails per se that the BCRs become legal obligations and, as such, may be enforced by the data subjects and the DPA. In any event, ‘authorised BCRs’ do not replace any obligation under the DP Regulations. To date, the DPA has authorised 16 BCRs related to the financial, insurance, consulting, pharma and technology sectors.

Turning to data localisation, there are no specific restrictions in Spain; however, along with the DP Regulations (which may impose restrictions on disclosing data to foreign government agencies and foreign courts, as explained in Section VI), there are specific laws imposing requirements that could be understood as ‘restrictive measures’, including, among others, tax regulations (Royal Decree 1619/2012 of 30 November on invoicing obligations), gambling regulations (Royal Decree 1613/2011) and specific public administration regulations (Law 9/1968 of 5 April on secrecy pertaining to official issues, Law 38/2003 of 17 November on subsidies and Law 19/2013 of 9 December on transparency and access to public information).

3 Case C-131/12.
4 The DPA’s prior authorisation is not required in the cases set out in Article 26 of EU Directive 95/46/EC.
V COMPANY POLICIES AND PRACTICES

Privacy and security policies
Organisations that process personal data are not required to have ‘general’ privacy policies, but they are useful for compliance with the information duties regarding processing activities (see Section III.ii). In addition, employees must be informed of the applicable security rules, and organisations must create and keep up to date a security document and a record of incidents (see Section IX).

Privacy officers
A chief privacy officer is not mandatory, but in practice this role is indispensable so that the controller or the processor can comply with the DP Regulations, in particular when the organisation is complex or the data processed are sensitive or private. In addition, one of the factors that may mitigate the liability in terms of breach is to have accountable data protection programmes, which necessarily entails the existence of the chief privacy officer. In any event, organisations must appoint a person responsible for the security measures for specific processing activities (in particular, but without limitation, the processing of data related to the rendering of financial services or of sensitive data).

In May 2018, when the GDPR obligations enter into force, several Spanish data controllers shall be required to appoint a data protection officer according to Article 37 of the GDPR. Although the draft of the new DP Law remains at a very preliminary stage, it expands the number of cases in which the appointment of a data protection officer will be mandatory.

Privacy impact assessments
Privacy impact assessments are not mandatory under the DP Regulations. Therefore, Spanish data controllers will not be obliged to carry them out until May 2018. However, the DPA has been encouraging the adoption of privacy impact assessments in certain cases (e.g., big-data projects) since 2014. In particular, in 2014, the DPA published guidelines on privacy impact assessments. The DPA is currently working on a new version of these guidelines, which is intended to be published at the end of 2017.

Work councils
Any employee representative in the organisation is entitled to issue a non-binding report before the implementation of new methods of control of the work. Although it is unclear what qualifies as a ‘method of control’ of the work, it is advisable to inform the works council of the implementation of new methods (e.g., whistle-blowing systems) and offer their members the possibility of issuing the above-mentioned non-binding report before its implementation.

VI DISCOVERY AND DISCLOSURE
Non-EU laws are not considered a legal basis for data processing, in particular regarding transfers to foreign authorities and especially if they are public authorities. This current approach is consistent with Article 6.3 of the GDPR.

E-discovery and any enforcement requests based on these laws require a complex case-by-case analysis from a data protection, labour and criminal law point of view (and other sector-specific regulations, such as bank secrecy rules).
From a data protection point of view, under the current DP Regulations, the main issues to be assessed include the need to obtain DPA authorisation, the lack of proportionality of requests, and whether information or consent is required. Some of these requirements (e.g., DPA authorisation) are expected to change once the new DP Law is approved. From labour and criminal law perspectives, privacy (rather than data protection) must be guaranteed.

In this regard, the international principles drawn up by the Sedona Conference have proven useful, in particular because Spain has filed reservations under Article 23 of the 1970 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters that essentially prohibit all pretrial document discovery.\(^5\)

### VII PUBLIC AND PRIVATE ENFORCEMENT

#### i Enforcement agencies

The DPA is the independent authority responsible for the enforcement of the DP Regulations\(^6\) and the data protection provisions of the LISS and the GTL.

Among other powers and duties, the DPA has powers that include the issuing of (non-binding) legal reports, recommendations, instructions and contributions to draft rules; powers of investigation; and powers of intervention, such as ordering the blocking, erasing or destruction of unlawful personal data, imposing a temporary or definitive ban on processing, warning or admonishing the controller or processor, or imposing administrative fines (fines are only imposed on private sector entities). The DP Regulations establish three classifications of infringements (and their correlative administrative fines): minor, serious and very serious. The fines for minor infringements are between €900 and €40,000; for serious infringements they are between €40,001 and €300,000; and for very serious infringements, the fines are between €300,001 and €600,000.

Disciplinary procedures start *ex officio*, but generally stem from a complaint submitted by any person (e.g., the data subject, consumer associations, competitors or former employees). These procedures must be settled within six months, and no other party may intervene in the proceedings. If a data subject considers him or herself to have been harmed by the conduct, he or she may claim damages (if duly evidenced) before the civil courts. The alleged infringer is entitled to lodge an appeal against the resolution either before the DPA itself (within one month) and, if not successful, before the administrative courts (within two months), or directly before the administrative courts (within two months).

The DPA will decide the final administrative fine, taking into account the mitigating and aggravating factors described in the law. In very limited cases, the DPA may decide not to start any penalty proceedings but to warn the liable entity, setting a term within which the entity must adopt corrective measures and evidence their implementation.

The DPA is very active: in addition to *ex officio* inspections of specific sectors (always announced in advance), in 2016 (the most recent official statistics published by the DPA): 10,583 investigations were carried out (18.49 per cent less than in 2015); 654 sanctioning resolutions were issued (15.61 per cent less than in 2015); and the fines amounted to approximately €14.2 million (3.48 per cent more than in 2015). Most of the sanctions

---

\(^5\) Article 23 specifically states that contracting states may declare, ‘at the time of signature, ratification or accession’, that they will not execute letters of request issued to obtain pretrial discovery of documents.

\(^6\) See footnote 2.
imposed on the private sector were for lack of consent and breach of the quality principle. The statistics show that the telecommunications, e-commerce and financial sectors are the top three sectors in terms of sanctions.

ii Recent enforcement cases

The following are the most significant enforcement issues to have arisen in Spain in the period 2016–2017.

The DPA has carried out numerous disciplinary proceedings related to the use of video-surveillance systems (170) and the disclosure of data to solvency and credit agencies (141). The DPA has also issued several resolutions assessing the application of the legitimate interest justification7 (e.g., in cases in which companies must comply with legal duties such as those related to the avoidance of conflicts of interest).

In addition, the number of proceedings carried out by the DPA against non-Spanish controllers has also increased. In fact, the DPA is participating in coordinated activities with other EU authorities to investigate companies that are based in the United States but carry out intensive processing activities in the EU.

Finally, the National Court recently handed down two judgments (dated 11 May 2017 and 19 June 2017) upholding the appeals lodged by Google Inc challenging specific DPA resolutions on the right to be forgotten; the judgments declared the DPA resolutions to be void. The first case related to specific negative comments regarding the professional performance of a doctor that were posted by a patient on a website; the second case assessed whether information related to the election of a politician in 2011 should or should not be removed. These represent the first judgments issued by the National Court regarding DPA resolutions issued against Google Inc in its role as a data controller.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before the civil courts. Claims for civil damages usually involve pecuniary or moral damages, or both, linked to the violation of honour (such as the improper disclosure of private information) and privacy rights (such as the dissemination of private images). In general, indemnities granted to date have been exceptional and have not exceeded €3,000 (with limited exceptions such as one awarding €20,000).

There are no specific class actions for data protection matters. However, consumer class actions have been used by consumer organisations to request that specific data protection clauses be overturned on the basis that they breach the DP Regulations.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The application of the DP Regulations for foreign organisations is triggered by either the existence of a data processor or processing equipment in Spain or, according to Google Spain, the existence of an establishment in Spain the activity of which is inextricably linked to that of the foreign organisation.

7 The legitimate interest justification is not expressly recognised by the DP Law.
In addition, online tracking and marketing activities addressed to the Spanish market may trigger the application of the data protection provisions of the LISS as well as the consumer regulations (only if consumers resident in Spain are involved), irrespective of where the organisation is established.

The major compliance issues that foreign organisations face relate to transfers outside the EEA, the information and consent rules, and security measures. However, the future application of the GDPR in Spain should facilitate foreign organisations’ compliance with local data protection requirements.

IX CYBERSECURITY AND DATA BREACHES

The approval in July 2016 of the NIS Directive was the most significant cybersecurity milestone in recent years. It marks the first instance of EU-wide rules on cybersecurity. The NIS Directive has not yet been implemented into Spanish law, although the government recently announced that a draft royal decree is being prepared (the content of which is not publicly available). Until implementation occurs, the regulation of cybersecurity matters in Spain will remain diffuse and insufficient, particularly in light of the steady rise in cybersecurity attacks involving Spanish organisations and infrastructure, such as the WannaCry and Petya cyberattacks. Furthermore, as a consequence of these recent attacks, the number of cybersecurity certifications has also increased. However, there has yet to emerge a clear market leader.

The DPA has also been highly active in relation to cybersecurity matters. Following the above-mentioned global attacks, the DPA published a post regarding ransomware attacks and how to guard against them. Among other recommendations, the DPA made the following key points: (1) companies should have a complex security plan for the protection of their networks (including a training plan for staff and the continuous updating of all software programs used by the company – especially those used for anti-virus purposes); (2) they should have an action plan for how to react in the event of an attack; and (3) they should have a remedial plan to be implemented once the attack is contained.

As to criminal law, the Spanish Criminal Code was amended in 2010 to implement the Convention on Cybercrime and Council Framework Decision 2005/222/JHA on attacks against information systems. Specifically, this entailed the introduction of two new criminal offences:

- the discovery and disclosure of secrets – namely, the unauthorised access to data or applications contained in an IT system – by any means and infringing implemented security measures; and
- the intentional deletion, damage, deterioration, alteration or suppression of data, applications and electronic documents of third parties rendering them unavailable, as well as the intentional serious hindering or interruption of the functioning of an information system.

Other criminal offences that could be related to cybercrime were also modified (computer fraud, sexual offences, technological theft, and offences against intellectual and industrial property). The Criminal Code was amended again in March 2015. Specifically, aligned with European regulations on computer-related offences, the following new criminal offences are regulated: (1) intercepting data from information systems for the discovery and disclosure of
secrets; and (2) creating computer programs or equipment for the purposes of discovering and disclosing secrets or committing damage to IT systems. Finally, legal entities can be held criminally liable for the above-mentioned offences.

Without prejudice to the above, there are no cybersecurity laws and requirements applicable to organisations ‘generally’, but rather a certain number of rules that address specific cybersecurity issues:

In 2012, the security breach notification regime was introduced in Spain through the GTL in line with Directive 2009/136/EC: the providers of public communications networks or publicly available electronic communications services must notify any security breaches, when personal data are involved, to both the data subjects and the DPA. In March 2014, the DPA approved an online system to notify security breaches. The requirements of the notification itself are those established in EU Regulation 611/2013. Since the notification of data breaches is not mandatory in general (except for the above-mentioned service providers), most of them remain unknown to the DPA and the public. One of those made public was the security breach suffered by BuyVip (which belongs to the Amazon group) in 2011, which involved the names, dates of birth, email addresses, phone numbers and shipping addresses of its customers. Although BuyVip was not subject to a notification duty in Spain, it decided to inform all its users of the security breach, and the notice went viral on the internet. The DPA then initiated an ex officio investigation, but the sanction imposed on BuyVip, if any, was not made public.

The LISS was amended in 2014 to establish specific obligations on cybersecurity incidents applicable to information society services providers, domain names registries and registrars. These obligations are twofold:

a to collaborate with the relevant computer emergency response teams to respond to cybersecurity incidents affecting the internet network (to this end, the relevant information – including IP addresses – must be disclosed to them, but ‘respecting the secrecy of communications’); and

b to follow specific recommendations on the management of cybersecurity incidents, which will be developed through codes of conduct (these have not yet been developed).

Operators of critical infrastructure 8 (entities responsible for investments in, or day-to-day operation of, a particular installation, network, system, physical or IT equipment designated as such by the National Centre for Critical Infrastructure Protection (CNPIC) under Law 8/2011) are subject to specific obligations, such as providing technological assistance to the Ministry of Home Affairs, facilitating inspections performed by the competent authorities, and creating the specific protection plan and the operator’s security plan.

Furthermore, these operators must appoint a security liaison officer and a security officer. The security liaison officer requires a legal authorisation (issued by the Ministry of Home Affairs), and his or her appointment must be communicated to this Ministry. The security officer does not need a legal authorisation, but his or her appointment must nevertheless be communicated to the relevant government delegation or the competent regional authority.

Royal Decree 3/2010 establishes the security measures to be implemented by Spanish public authorities to ensure the security of the systems, data, communications and e-services

8 The following infrastructure areas have been considered ‘critical’ by Law 8/2011 (which transposes Directive 2008/114/EC into Spanish law): administration, water, food, energy, space, the chemical industry, the nuclear industry, research facilities, health, the financial and tax system, ICT and transport.
addressed to the public, and they could apply by analogy. These security measures are classified into three groups: the organisational framework, which is composed of the set of measures relating to the overall organisation of security; the operational framework, consisting of the measures to be taken to protect the operation of the system as a comprehensive set of components organised for one purpose; and protection measures, focused on the protection of specific assets according to their nature, and the required quality according to the level of security of the affected areas. Spanish law does not directly address restrictions to cybersecurity measures.

Although cybersecurity requirements do not specifically refer to personal data (but rather to any kind of information), the security measures of RD 1720/2007 apply when personal data are involved, which distinguishes between three levels of security measures depending on the nature of the data.

Among other security measures, an incidents register must be established. In addition, public and private organisations that process specific personal data must appoint a security officer to monitor compliance with the personal data security requirements. No specific legal rules apply to this appointment. The skills of this security officer and the resources and powers allocated to him or her within the organisation must be appropriate to ensure that the organisation complies with the legally prescribed security requirements.

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as:

- the guidelines published by the Spanish National Institute of Cybersecurity (INCIBE) in 2015 regarding, inter alia:
  - how companies should manage information leaks;
  - cybersecurity on e-commerce;
  - security-related risk management for companies; and
  - protocols and network security in industrial control systems infrastructures;
- the publication by INCIBE in 2016 of a consolidated code of cybersecurity rules in Spain;
- the National Cybersecurity Strategy issued by the presidency in 2013;
- the strategy series on cybersecurity issued by the Ministry of Defence; and
- the Supervisory Control and Data Acquisition Guidelines issued by the CNPIC in collaboration with the National Cryptological Centre (CNN) in 2010.

The agencies and bodies with competences on cybersecurity are numerous:

- the CCN, which is part of the National Intelligence Centre;
- the CCN Computer Emergency Response Team;
- the CNPIC;
- the Cybersecurity Coordinator’s Office (which is part of the CNPIC);
- the Secretary of State for Telecommunications and Information Society; and
- INCIBE (previously known as the National Institute of Communication Technologies), which is the public sector company in charge of developing cybersecurity.

X OUTLOOK

Data protection is constantly evolving. In the past, it has been neglected by both private and public organisations or deemed an unreasonable barrier for the development of the economy. However, this trend has definitively changed in the past five years.
This change is mostly due to the sanctions imposed by the DPA, the role of data in the development of the digital economy (the ‘new oil’), the active voice of users in the digital environment (developing new social interactions and not only acting as consumers) and the fact that the European Commission and the European Parliament have definitively embraced a strong ‘privacy mission’. Decisions of the CJEU (such as declaring the Data Retention Directive 2006/24/EC invalid, also declaring the Safe Harbor scheme invalid, and the application of the Spanish data protection law to Google Inc through a wide and economic construction of the concept of ‘establishment’) have also sent out a clear message on the importance of data protection rules in Europe.

The adoption in 2016 of the GDPR constituted a significant milestone in the construction of a new data protection environment. In Spain, the government is working hard to approve the new DP Law before the mandatory deadline (May 2018). Although the GDPR is actually fairly similar to the current DP Regulations, as construed by the CJEU and the Article 29 Working Party, Spanish organisations are particularly concerned about the new fines (the applicable criteria for which would be similar to those used in antitrust regulations – a percentage of annual worldwide turnover), the accountability principle, the general security breach notification and the mandatory implementation of a data protection officer. Additional requirements regarding information and consent duties set out in the GDPR will also be a challenge for Spanish data controllers.
Chapter 25

SWITZERLAND

Jürg Schneider, Monique Sturny and Hugh Reeves

I OVERVIEW

Data protection and data privacy are fundamental constitutional rights protected by the Swiss Constitution. Swiss data protection law is set out in the Swiss Federal Data Protection Act of 19 June 1992 (DPA) and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 14 June 1993 (DPO). Further data protection provisions governing particular issues (e.g., the processing of employee or medical data) are spread throughout a large number of legislative acts. As Switzerland is neither a member of the European Union (EU) nor of the European Economic Area (EEA), it has no general duty to implement or comply with EU laws. Accordingly, Swiss data protection law has some peculiarities that differ from the data protection laws of most EU Member States. However, because of Switzerland’s location in the centre of Europe and its close economic relations with the EU Member States, Swiss law is in general strongly influenced by EU law, both in terms of content and interpretation. A closer alignment of Swiss data protection law with the EU data protection provisions is also one of the aims of the ongoing reform of the DPA, which the Swiss Federal Council initiated in April 2015.

The Swiss Data Protection and Information Commissioner (Commissioner) is the responsible authority for supervising both private businesses and federal public bodies with.

1 Jürg Schneider is a partner and Monique Sturny and Hugh Reeves are associates at Walder Wyss Ltd.
2 Classified compilation (SR) 235.1, last amended as of 1 January 2014.
3 Classified compilation (SR) 235.11, last amended as of 16 October 2012.
4 Specific duties exist in certain areas based on international treaties. Furthermore, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation (GDPR)), which will apply from 25 May 2018, is not only relevant for companies located in EU and EEA Member States, but also for Swiss companies under certain circumstances, as it applies, inter alia, to data processing activities outside the EU and EEA that have effects in the EU or EEA (the effects doctrine). In particular, the GDPR applies to Swiss companies in connection with the targeted offering of goods or services to persons in the EU and EEA or the monitoring of behaviour of persons in the EU and EEA (Article 3 GDPR). In addition, the GDPR may become applicable if a person with habitual residence in the EU or EEA were to claim the applicability of the law of its state of habitual residence based on Article 139 Paragraph 1 Letter (a) of the Swiss Federal Act on Private International Law of 18 December 1987 (PILA, Classified compilation [SR] 291, last amended as of 1 April 2017) or, if the effects of an infringement of personality rights through the processing of personal data occurred in the EU or EEA, the injured person may claim the applicability of the law of the state in which the effects of the damaging act occurred and the infringing party should have foreseen that the effects would occur in that state (Article 139 Paragraph 1 Letter (b) and Paragraph 3 PILA).
respect to data protection matters. The Commissioner has published several explanatory
guidelines that increase legal certainty with respect to specific issues such as data transfers
abroad, technical and organisational measures, processing of data in the medical sector
and processing of employee data.⁵ Despite the lack of drastic sanctions in respect of data
protection under the current legislative regime, it is nonetheless a topic at the forefront of
public attention in Switzerland, especially given the active presence of the Commissioner and
the high level of media attention given to data protection matters.

II THE YEAR IN REVIEW

Of a number of noteworthy reforms initiated back in 2015, some are still pending and some
are expected to enter into force shortly or entered into force recently.

On 1 April 2015, the Swiss Federal Council formally decided to undertake a revision
of the DPA, which is still ongoing. On 21 December 2016, the Federal Council issued
a preliminary draft of the revised DPA. This preliminary draft was subject to a public
consultation process, which ended on 4 April 2017 and, in late August 2017, the Federal
Council released the results and the various opinions gathered throughout the consultation
process. This in turn resulted in the establishment of a revised draft accompanied by an
explanatory report of the Swiss Federal Council on 15 September 2017.⁶ The draft for
a revised DPA will now be subject to parliamentary discussion. Once the revision has been
approved by the parliament, it may still be challenged by an optional referendum. Entry into
force of the revised DPA is tentatively scheduled for 1 August 2018 at the earliest.

The aim of the ongoing reform of the DPA is – among others – to lay the foundations
for Switzerland’s ratification of the modernised Council of Europe Convention for the
Protection of Individuals with regard to Automatic Processing of Personal Data (Convention
108) and, where necessary in the context of the further development of the Schengen/Dublin
acquis, the adaptation of the DPA to the EU data protection provisions (see Section X, for
more details).

On 31 August 2016, the Swiss Federal Council approved the transposition into Swiss
law of the regulation contained in the new EU Directive dated 27 April 2016 (EC 2016/680)
regarding data protection in the field of criminal prosecution as well as police and judicial
cooperation. This Directive contains rules on data processing, strengthens the protection of
individuals, and sets out the requirements for a transfer of personal data from a Schengen
Member State to third countries or international organisations. The necessary changes to
the DPA and other Swiss laws in this respect will be made as part of the currently ongoing
revision of the DPA.

The revision process of the Swiss Federal Act on the Supervision of Postal and
Telecommunication Services was successfully terminated, and the revised Act and the revised

⁵ The guidelines are not legally binding, but do set de facto standards.
⁶ The draft DPA, the explanatory report of the Swiss Federal Council and the summary of the results of the
consultation process are available in German, French and Italian on the website of the Swiss Confederation
at: (in German) www.ejpd.admin.ch/epjd/de/home/aktuell/news/2017/2017-09-150.html; (in French)
admin.ch/epjd/it/home/aktuell/news/2017/2017-09-150.html (all sites last visited on 27 September 2017).
An unofficial English translation of the draft DPA can be found at: https://www.dataprotection.ch/
dpa-revision/documentation-and-english-translation/.
related ordinance entered into force on 1 September 2017. The main changes concern in particular the monitoring of new technologies, the tasks of the competent authority, the personal scope of application and the storage of data.

The new Swiss Federal Act on Intelligence Service (the Intelligence Service Act) was approved in a referendum in September 2016 and entered into force, together with its related ordinance, on 1 September 2017. The new Intelligence Service Act will bring increased monitoring competence for Swiss intelligence services and was predominantly driven by increased efforts to prevent terrorism. The expansion of surveillance options has been heavily debated and criticized for undermining privacy and other fundamental rights of data subjects.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

The Swiss Constitution of 18 April 1999 guarantees the right to privacy in Article 13. The federal legislative framework for the protection of personal data mainly consists of the DPA and the DPO. Further relevant data protection provisions are contained in the Federal Ordinance on Data Protection Certification of 28 September 2007. Specific data protection issues such as, inter alia, transfers of data abroad, and data protection in relation to employees or as regards the medical sector, are dealt with in more detail in the relevant guidelines published by the Commissioner.

Key definitions under the DPA

a Personal data (or data): all information relating to an identified or identifiable person. Unlike the data protection laws of most other countries, Swiss data protection law currently protects personal data relating to both individuals and legal entities. Hence, the term ‘person’ refers not only to natural persons (individuals), but also to legal entities such as corporations, associations, cooperatives or any other legal entity, as well as partnerships. It is likely, however, that personal data relating to legal entities will no longer be protected under the revised DPA.
b Data subject: an individual or, currently, also a legal entity whose data is being processed.
c Processing of personal data: any operation with personal data, irrespective of the means applied and the procedure, and in particular the storage, use, revision, disclosure, archiving or destruction of data.

7 Classified compilation (SR) 780.1 and SR 780.11.
8 BBl 2013 2686.
9 Classified compilation (SR) 121 and SR 121.1.
10 Classified compilation (SR) 101, last amended as of 12 February 2017.
11 The federal legislative framework exclusively applies to the processing of personal data by private persons and federal bodies. Processing of personal data by Swiss cantonal bodies is governed by the specific and distinct data protection legislation of each of the 26 cantons. Unless explicitly set forth otherwise, this overview does not address the particularities of the data protection legislation at the cantonal level.
12 Classified compilation (SR) 235.13, last amended as of 1 November 2016.
13 As mentioned in footnote 5, the guidelines are not legally binding, but do set de facto standards.
14 Article 3 DPA.
d Sensitive personal data: data relating to:
• religious, ideological, political or trade union-related views or activities;
• health, the intimate sphere or racial origin;
• social security measures; and
• administrative or criminal proceedings and sanctions.

e Personality profile: a collection of data that permit an assessment of essential characteristics of the personality of a natural person. Swiss data protection law provides an enhanced data protection level for personality profiles, similar to the protection of sensitive personal data. It is likely that the term will be replaced by the term ‘profiling’ under the revised DPA, bringing a closer alignment to corresponding EU provisions.

f Data file: any set of personal data that is searchable by data subject. It is likely that this term will no longer be used under the revised DPA.

g Controller of the data file: the controller of the data file is the private person or federal body that decides on the purpose and content of a data file (the term ‘controller’ is likely to be used under the revised DPA, bringing a closer alignment to the corresponding EU provisions).

As mentioned, it is likely that some terms will change under the revised data protection regime. In particular, it appears likely that ‘profiling’ will replace the term ‘personality profiles’ and the concepts of ‘data file’ and ‘controller of the data file’ will no longer be used in the revised DPA. However, as the final text of the revised DPA has not yet been adopted, it is too early to give conclusive indications as to the changes that will in fact occur.

ii General obligations for data handlers

Anyone processing personal data must observe the following general obligations.15

Principle of good faith

Personal data must be processed in good faith. It may not be collected by misrepresentation or deception.

Principle of proportionality

The processing of personal data must be proportionate. This means that the data processing must be necessary for the intended purpose and reasonable in relation to the infringement of privacy. Subject to applicable regulations on the safekeeping of records, personal data must not be retained longer than necessary.

Principle of purpose limitation

Personal data may only be processed for the purpose indicated at the time of collection, unless the purpose is evident from the circumstances or the purpose of processing is provided for by law.

Principle of transparency

The collection of personal data, and in particular the purposes of its processing, must be evident to the data subject concerned. This principle does not always lead to a specific

15 Articles 4, 5 and 7 DPA.
disclosure obligation, but it will be necessary to give notice of any use of personal data that is not apparent to the data subject from the circumstances. For example, if personal data are collected in the course of concluding or performing a contract, but the recipient of the personal data intends to use the data for purposes outside the scope of the contract or for the benefit of third parties, then those uses of the personal data must be disclosed to the data subject.

**Principle of data accuracy**
Personal data must be accurate and kept up to date.

**Principle of data security**
Adequate security measures must be taken against any unauthorised or unlawful processing of personal data, and against intentional or accidental loss, damage to or destruction of personal data, technical errors, falsification, theft and unlawful use, unauthorised access, changes, copying or other forms of unauthorised processing. If a third party is engaged to process personal data, measures must be taken to ensure that the third party processes the personal data according to the given instructions and that the third party implements the necessary adequate security measures.

Detailed technical security requirements for the processing of personal data are set out in the DPO.

**Principle of lawfulness**
Personal data must be processed lawfully. This means that the processing of personal data must not violate any Swiss legislative standards, including any normative rules set forth in acts other than the DPA that directly or indirectly aim at the protection of the personality rights of a data subject.

**Processing personal data does not necessarily require a justification**
According to the Swiss data protection regime, the processing of personal data does not per se constitute a breach of the privacy rights of the data subjects concerned. Accordingly, processing in principle only requires a justification if it unlawfully breaches the privacy of the data subjects (Article 12 Paragraph 1 in relation to Article 13 DPA).

In general, no justification for processing personal data is required if the data subjects have made the data generally available and have not expressly restricted the data processing (Article 12 Paragraph 3 DPA). On the other hand, a justification is required particularly if the processing violates one of the general data protection principles of the DPA outlined above, if the personal data is processed against the data subjects’ express wish, or if sensitive personal data or personality profiles are disclosed to third parties for the third parties’ own purposes (Article 12 Paragraph 2 DPA).

If a justification for processing is required, the justification exists if the data subject has consented to it, Swiss (federal, cantonal and municipal) law provides for it, or there is an overriding private or public interest in the data processing (Article 13 Paragraph 1 DPA).

---

16 The public interest justification must exist from a Swiss perspective. However, this does not only include Swiss public interests. Supporting foreign concerns – depending on the circumstances – may also qualify as a public interest from a Swiss perspective. This needs to be checked on a case-by-case basis.
According to Article 13 Paragraph 2 DPA, an overriding private interest of the data handler shall be considered in particular if he or she:

- processes personal data in direct connection with the conclusion or the performance of a contract and the personal data in question are the data of one of the contractual parties;
- competes for business with, or wants to compete for business with, another person and processes personal data for this purpose without disclosing the data to third parties for the third parties’ own purposes;
- processes data that are neither sensitive personal data nor a personality profile to verify the creditworthiness of another person, and discloses the data to third parties for the third parties’ own purposes only if the data are required for the conclusion or the performance of a contract with the data subject;
- processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;
- processes personal data for purposes that are not related to a specific person, in particular research, planning or statistics, and the results are published in a manner that does not permit the identification of the data subjects; or
- collects personal data about a person who is a public figure to the extent that the personal data relates to the role of the person as a public figure.

The fact that a data handler has one of the above-listed interests in processing personal data does not mean per se that the data handler has an overriding interest in processing the personal data. The interest of the data handler in processing the personal data must always be weighed against the interest of the data subject in being protected against an infringement of his or her privacy. Only in situations where the interest of the data handler outweighs the interest of the data subject is the processing of personal data justified by the overriding interest of the data handler.

**Consent**

Under Swiss data protection law, processing of personal data does not require consent of the data subject concerned in all instances. However, as mentioned above, consent of the data subject may constitute a possible justification for data processing that would otherwise be unlawful (e.g., because of an infringement of the principles outlined above, or in the event of a disclosure of sensitive personal data or personality profiles to third parties for the third parties’ own purposes). To the extent that the legality of data processing is based on the consent of the data subject concerned, the consent is only valid if given voluntarily upon provision of adequate information. In the case of processing sensitive personal data or personality profiles, the consent must be given expressly (Article 4 Paragraph 5 DPA).

**Registration**

Controllers of data files that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties (including affiliates), must register their data files with the Commissioner before they start processing the data (Article 11a DPA). The Commissioner maintains a register of data files that have been registered in this manner that is accessible online. If a controller is required to register, it becomes subject to additional

---

17 Cf. Article 12 Paragraph 2 Letter (c) DPA.
documentary obligations. There are several exceptions to the duty to register data files. *Inter alia*, no registration is required if the controller of the data file is obliged by Swiss law to process the data in question (e.g., in the case of an employer processing employee data for Swiss social security purposes) or has nominated its own independent data protection officer monitoring the data protection compliance of the data controller. Several further exceptions are set forth in Article 11a Paragraph 5 DPA and Article 4 Paragraph 1 DPO.

It is likely that the revised DPA will no longer contain such a registration duty and will instead introduce documentation requirements for both controllers and processors.

### iii Technological innovation and privacy law

#### Automated profiling and data mining

The legality of automated profiling and data mining is doubtful under Swiss data protection law, as such practices inherently involve the use of personal data for a range of purposes, some of which may not have been disclosed when the personal data was collected. Hence, such practices may constitute an unlawful breach of privacy because of an infringement of the principles of transparency, purpose limitation and proportionality unless justified by law, an overriding public or private interest or consent.

#### Cloud computing

Cloud computing raises various data protection issues. The Commissioner has issued a guide pointing out the risks and setting out the data protection requirements when using cloud computing services.18

In particular, the processing of personal data may only be assigned to a cloud service provider if the assignment is based on an agreement or on the law, if the personal data is processed by the cloud service provider only in the manner permitted for the assignor, and if the assignment is not prohibited by a statutory or contractual duty of confidentiality (Article 10a Paragraph 1 DPA). Furthermore, the assignor must ensure that the cloud service provider guarantees data security (Article 10a Paragraph 2 DPA). The assignor must in particular ensure that the cloud service provider ensures the confidentiality, availability and integrity of the personal data by taking adequate measures against unauthorised processing through adequate technical and organisational measures (see Article 7 DPA and Article 8 et seq. DPO). Additionally, if cloud computing services involve disclosures of personal data abroad, the specific requirements for transborder data flows must be complied with (see Section IV). Finally, the assignor must also ensure that, despite the use of a cloud service provider, the data subjects may still exercise their right to information (Article 8 DPA), and may demand deletion or correction of data in accordance with Article 5 DPA.

#### Big data

From an economic point of view, big data has great potential. In particular, big data offers new opportunities for social and scientific research. However, big data may threaten privacy if the processed data is not or is inadequately anonymised. In fact, the DPA is not applicable to fully and completely anonymised data. However, if the processing of big data involves the processing of data that has not been fully and completely anonymised (e.g., because it

---

can be ‘de-anonymised’ at a later stage by merging different data files), the right to privacy and the protection of personal data need to be guaranteed. The use of big data that is not entirely anonymised and the general data protection principles of the DPA are potentially conflicting, particularly with regard to the principles of purpose limitation, proportionality and transparency (see Section III.ii).

**Cookies**

Since 2007, the use of cookies has been regulated in Article 45c Letter (b) of the Telecommunications Act of 30 April 1997. According to this Article, website operators have to inform users about the use of cookies and its purpose. Furthermore, they need to explain how cookies can be rejected (i.e., how cookies can be deactivated in the user’s browser). Switzerland basically follows the opt-out principle.

**Drones**

In Switzerland, in general, drones of up to 30 kilograms do not require a specific permit, as long as they do not overly crowd people and provided that the ‘pilot’ has visual contact with the drone at all times. Nowadays drones are usually equipped with cameras. As a result, people using drones need to comply with data protection regulations as soon as they view or record identified or identifiable persons. To the extent that such viewing or recording constitutes an unlawful breach of the privacy of the data subjects concerned, it needs to be justified either by the consent of the injured party, by an overriding private or public interest or by law (Article 13 Paragraph 1 DPA).

### iv Specific regulatory areas

**Processing of employee data in general**

Article 328b of the Swiss Code of Obligation (CO) applies in addition to the DPA to the processing of personal data of employees.

> According to Article 328b CO, the employer may process personal data concerning an employee only to the extent that the personal data concerns the employee's suitability for his or her job or is necessary for the performance of the employment contract. Article 328b CO is mandatory, and any deviation from this provision to the disadvantage of the employee is null and void (Article 362 CO).

---

19 Classified compilation (SR) 784.10, last amended as of 1 September 2017.
21 It must further be noted that, according to Article 179 quater CC, a person who, without consent, observes with a recording device or records with an image-carrying device information from the secret domain of another person or information from the private domain of another person that is not readily available to everyone is criminally liable; see also Commissioner, ‘Video surveillance with drones by private persons’, available at www.edoeb.admin.ch/datenkutz/00625/00729/01171/index.html?lang=de (status 2014; in German; no English version available; last visited on 27 September 2017).
22 Some legal authors, however, hold that an employee may specifically and unilaterally consent (i.e., not in the employment contract or in any other agreement with the employer) to the processing of personal data that goes beyond Article 328b CO.
Furthermore, Article 26 of Ordinance 3 to the Employment Act\textsuperscript{23} prohibits the use of systems that monitor the behaviour of employees, except if the monitoring systems are necessary for other legitimate reasons (e.g., quality control, security requirements, technical reasons) and provided that the systems do not impair the health and mobility of the employees concerned. If monitoring is required for legitimate reasons, it must at all times remain proportionate (i.e., limited to the extent absolutely required) and the employees must be informed in advance about the use of monitoring systems. Permanent monitoring is in general not permitted.

The Commissioner has issued specific guidelines with respect to the processing of employee data.\textsuperscript{24}

**Monitoring of internet and email use by employees**

As regards monitoring of internet and email use by employees in particular, the following requirements apply:

\begin{itemize}
  \item[a] the employer shall issue a ‘use policy’ that describes the permitted uses the employee may make of company internet and email resources;
  \item[b] constant individual analysis of log files is not allowed;
  \item[c] permanent anonymous analysis of log files and random pseudonymised analysis are admissible to verify whether the use policy is complied with;
  \item[d] individual analysis of log files is only allowed if the employee has been informed in advance of this possibility (e.g., in a ‘monitoring policy’) and if misuse has been detected or there is a strong suspicion of misuse; and
  \item[e] the monitoring policy must particularly indicate the possibility of an individual analysis, the possibility of forwarding the analysis to the HR department in the event of misuse and any possible sanctions.
\end{itemize}

As a general rule, employers shall not read any employee emails that have private content (even if misuse has been established). In the event of specific suspicion of a criminal offence, evidence may, however, be saved, and the employer may refer to the criminal prosecution authorities for further prosecution.

**Whistle-blowing hotlines**

The use of whistle-blowing hotlines is not specifically regulated by the DPA or the CO. Hence, the general rules, in particular on data and employee protection, apply. In a nutshell and from a DPA and CO perspective, whistle-blowing hotlines can be used if certain minimum requirements are met, such as, *inter alia*:

\begin{itemize}
  \item[a] the transparent informing of employees, contractors, etc., about the existence of the whistle-blowing hotline;
  \item[b] the informing of relevant employees, contractors, etc., of allegations about them contained in a specific whistle-blowing report, unless there is an overriding interest not to do so to protect the ensuing investigations or the reporting person;
\end{itemize}

\textsuperscript{23} Ordinance 3 to the Employment Act (Healthcare) of 18 August 1993, last amended as of 1 October 2015, classified compilation (SR) 822.113.

adequate safeguards to protect the data subjects from false or slanderous accusations; and

strong state-of-the-art security measures.

However, it is important to verify compliance on an individual basis before implementing a whistle-blowing hotline. In particular, and unless an exception applies, whistle-blowing hotlines (and the underlying data files, respectively) may require prior registration with the Commissioner (see Section III.ii), and in the event of transfers abroad, specific requirements must be met (see Section IV). Furthermore, and in particular in a cross-border context, whistle-blowing hotlines may be impacted by blocking statutes.

Bring your own device (BYOD)

Using BYOD causes data protection concerns because of the difficulty in separating private and business data. The Commissioner recommends respecting the following rules while using BYOD:

a establish clear use regulations about what is allowed and what is prohibited;

b maintain a separation of business and private data (both technical and logical);

c ensure data security (e.g., through encryption or passwords);

d establish clear regulations on where the business data are stored;

e use of employees’ own devices must be approved in advance by a person responsible within the company; and

f establish clear regulations regarding access to the device by the employer.25

IV INTERNATIONAL DATA TRANSFER

Any disclosure of personal data from Switzerland to countries abroad must comply with the DPA. A disclosure of data abroad occurs when personal data are transferred from Switzerland to a country outside Switzerland or when personal data located in Switzerland are accessed from outside Switzerland. The DPA prohibits a disclosure of personal data abroad if the transfer could seriously endanger the personality rights of the data subjects concerned. Such a danger may in particular occur if the personal data are disclosed to a country whose legislation does not guarantee an adequate protection for personal data.

The Commissioner has published a (non-binding) list of countries that provide an adequate data protection level with respect to individuals.26 As a rule, the countries that have implemented EU Directive 95/46/EC are considered to provide an adequate data protection level relating to individuals.27 However, according to the list, most of these countries do not provide an adequate data protection level with respect to data relating to legal entities.


27 It is expected that this situation will remain unchanged upon the entry into force of the GDPR.
With respect to data transfers to non-EU or non-EEA countries, it is necessary to check on a case-by-case basis whether the country provides an adequate level of data protection with respect to personal data pertaining to individuals and legal entities. The same applies for transfers of personal data relating to legal entities to EU or EEA countries.\(^28\)

If personal data are to be transferred to a country that does not provide an adequate data protection level for the personal data being transferred, the transfer may only occur if (Article 6 Paragraph 2 DPA):

\(a\) sufficient safeguards, in particular contractual clauses (typically EU Model Contract Clauses adapted to Swiss law requirements), ensure an adequate level of protection abroad;

\(b\) the data subject has consented in an individual specific case;

\(c\) the processing is directly connected with the conclusion or the performance of a contract and the personal data are that of a contractual party;

\(d\) disclosure is essential in specific cases to either safeguard an overriding public interest, or for the establishment, exercise or enforcement of legal claims before the courts;

\(e\) disclosure is required in the specific case to protect the life or the physical integrity of the data subject;

\(f\) the data subject has made the data generally accessible and has not expressly prohibited its processing; or

\(g\) disclosure is made within the same company or the same group of companies, provided those involved are subject to data protection rules that ensure an adequate level of protection (i.e., that have adopted binding corporate rules, BCR).

In addition, in the case of the exceptions mentioned under \((a)\) and \((g)\) above, the Commissioner must be informed in advance (i.e., before the transfer takes place) about the safeguards that have been taken or the BCR that have been adopted. If the safeguards consist of EU Model Contract Clauses adapted to Swiss law requirements or other contractual clauses explicitly accepted by the Commissioner,\(^29\) then it is sufficient to inform the Commissioner that such clauses have been entered into, and there is no need to actually submit the clauses to the Commissioner for review. As regards information about BCR, it is common practice to submit a copy of the rules to the Commissioner (including, if applicable, a copy of a letter of the coordinating EU Member State’s data protection authority authorising the BCR on an EU level).

On 11 January 2017, the Swiss Federal Council announced the establishment of the US–Swiss Privacy Shield. This framework is separate from – but closely resembles – the US–EU Privacy Shield (which was formally adopted by the European Commission on 16 July 2016 and predates the US–Swiss Privacy Shield). It replaces the former US–Swiss Safe Harbor Framework and purports to facilitate the transfers of personal data from Switzerland to the United States. Indeed, since 12 April 2017, companies based in the United States

\(^{28}\) It can, in our view, be reasonably argued that the fact that most EU or EEA member countries’ data protection legislation does not specifically protect personal data pertaining to legal entities does not per se result in an absence of adequate protection. The protection for such data may also be adequate based on other legislation. Furthermore, the transfer of personal data pertaining to legal entities does not necessarily seriously endanger the legal entity’s personality rights.

have been able to self-certify under the US–Swiss Privacy Shield. For a company certified under the US–Swiss Privacy Shield an adequate level of data protection is deemed to exist for the personal data covered by the certification. Hence personal data may be transferred from Switzerland to a company based in the United States that is certified under the US–Swiss Privacy Shield even if none of the exceptions set forth in Article 6 Paragraph 2 DPA apply. As mentioned above, the US–Swiss Privacy Shield is separate from the US–EU Privacy Shield. For transfers from Switzerland to the United States, the certification under the US–Swiss Privacy Shield is relevant and a certification only under the US–EU Privacy Shield is not sufficient.

V COMPANY POLICIES AND PRACTICES

According to Article 11 Paragraph 1 DPA, the private controller of an automated data file subject to registration under Article 11a Paragraph 3 DPA that is not exempted from the registration requirement under Article 11a Paragraph 5 Letters (b)–(d) DPA shall issue a processing policy that describes in particular the internal organisation, data processing and control procedures, and that contains documentation on the planning, realisation and operation of the data file and the information technology used. This policy must be updated regularly and made available upon request to the Commissioner.

Other than in the aforementioned case, the DPA does not explicitly require private personal data handlers to put in place any specific policies as regards the processing of personal data. However, for private personal data handlers to effectively ensure compliance with substantive and formal data protection requirements, it has become best practice for large and medium-sized companies to adopt and implement various policies in this area. In particular, the following policies (either in separate or combined documents) are recommended:

- a policy regarding the processing of job applicant and employee personal data (including a policy that governs the use by employees of the company’s information technology resources, monitoring by the employer of employees’ use of those resources and possible sanctions in the event of misuse, rules on BYOD, etc.);
- a policy regarding the processing of customer personal data;
- a policy regarding the processing of supplier personal data;
- a whistle-blowing policy;
- a policy or privacy notice for collecting and processing personal data on a company’s websites;
- a policy on data and information security (qualification of data according to risk, required measures per risk category, access rights, procedures in the event of data breaches, internal competence, etc.); and
- a policy on archiving of personal data and record-keeping (including guidelines on how long different categories of data must be stored).

30 The dedicated Privacy Shield Framework website sets up this process: www.privacyshield.gov/welcome (last visited on 27 September 2017). It also allows any interested person to consult the list of certified companies: www.privacyshield.gov/list.

31 Federal public controllers of data files have a similar obligation to issue a processing policy for automated data files that contain sensitive personal data or personality files, are used by two or more federal bodies, are disclosed to third parties or are connected to other data files (see Article 21 DPO).
In contrast to other countries’ legislation, the DPA does not require private data handlers to appoint a data protection officer. For this reason, and until a few years ago, companies’ data protection officers have not played a very important role in Switzerland compared with their role in other countries. However, in the past few years, more and more medium-sized and large companies domiciled in Switzerland have chosen to appoint a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files of the company in question. In fact, appointing such a data protection officer is one way for private data controllers to avoid having to register data files with the Commissioner that otherwise would have to be registered under the current regime (see Article 11a Paragraph 3 DPA in relation to Article 11a Paragraph 5 Letter (e) DPA; see also Section III.ii). Currently, over 1,000 companies have notified the Commissioner of their appointment of an independent data protection officer.

BCR ensuring an adequate level of protection of personal data on a group-wide level facilitate the cross-border disclosure of personal data among group companies (see Section IV). Despite this fact, and until recently, BCR have not been used very frequently in Switzerland. In the past few years, however, there has been a noticeable increase in the number of large companies adopting BCR and informing the Commissioner accordingly. We expect this number to further increase in the next few years.

VI DISCOVERY AND DISCLOSURE

In Switzerland, the taking of evidence constitutes a judicial sovereign function of the courts rather than of the parties. Therefore, taking evidence for a foreign state court or for foreign regulatory proceedings constitutes an act of a foreign state. Such acts, if they take place in Switzerland, violate Swiss sovereignty and are prohibited by Article 271 of the Swiss Criminal Code of 21 December 1937 (CC) unless they are authorised by the appropriate Swiss authorities or are conducted by way of mutual legal assistance proceedings. A violation of Article 271 CC is sanctioned with imprisonment of up to three years or a fine of up to 1.08 million Swiss francs, or both. It is important to note that transferring evidence outside Switzerland for the purposes of complying with a foreign country’s order requiring the production of evidence does not prevent an application of Article 271 CC. Moreover, Switzerland does not accept ‘voluntary’ production of evidence even if foreign procedural laws require such production. Therefore, evidence may only be handed over to foreign authorities lawfully by following mutual legal assistance proceedings or by obtaining authorisation from the competent Swiss authorities. If one is requested to produce evidence in a foreign court or in regulatory proceedings by way of pending mutual legal assistance proceedings, the DPA does not apply to the production (Article 2 Paragraph 2 Letter (c) DPA). As a consequence, and in particular, evidence containing personal data may in such cases be disclosed abroad to foreign parties or authorities located in countries without adequate protection of personal data without having to comply with the restrictions set forth in Article 6 DPA.

32 The DPA also does not apply to pending Swiss civil proceedings, pending Swiss criminal proceedings and pending Swiss proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance (see Article 2 Paragraph 2 Letter (c) DPA).

33 In contrast, producing and taking evidence in purely private foreign arbitral proceedings is not subject to Article 271 CC and therefore do not require that the parties follow the requirements of mutual legal assistance proceedings. However, as the DPA fully applies to the processing of personal data in
In addition to Article 271 CC, Article 273 CC prohibits industrial espionage of manufacturing and business secrets by foreign official agencies, foreign organisations, foreign private enterprises or their agents. Accordingly, manufacturing and business secrets with sufficient connection to Switzerland may only be released or communicated abroad when:

- the owner of the secret relinquishes its intent to keep the information secret;
- the owner of the secret agrees to disclose this information;
- all third parties (who have a justifiable interest in keeping the information secret) consent to such a disclosure;
- Switzerland has no immediate sovereign interest in keeping the information secret; and
- all requirements set forth by the DPA (in particular as regards cross-border transfers) are complied with.

However, Article 273 CC does not apply in cases in which Swiss authorities have granted mutual legal assistance and disclosure takes place in accordance with the proceedings. Contrary to Article 271 CC, Article 273 CC can also be violated by activities taking place outside Switzerland.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner supervises compliance of both federal bodies and private persons (individuals and legal entities) with the DPA, DPO and other federal data protection regulations. The Commissioner fulfils these tasks independently without being subject to the directives of any authority.

For this purpose, the Commissioner may investigate cases either on his or her own initiative or at the request of a third party. The Commissioner may request the production of files, obtain information and request that a specific instance of data processing is demonstrated to him or her. If such an investigation reveals that data protection regulations are being breached, the Commissioner may make recommendations as to how the method of data processing shall be changed or that the data processing activity shall be stopped. If such a recommendation is not complied with, the Commissioner may initiate proceedings leading to a formal decision on the matter.

In the case of recommendations to federal bodies, the Commissioner may refer the case to the competent department or the Swiss Federal Chancellery for a formal decision. Both the Commissioner and any persons concerned by such a decision may file an appeal against the decision with the Swiss Federal Administrative Court. The appeal decision can be appealed to the Swiss Federal Supreme Court.

---

[34] The processing of personal data by cantonal and communal bodies is regulated by cantonal law (see footnote 11). Each canton has a cantonal data protection authority, be it a cantonal data protection officer or a commission competent for cantonal and communal data protection matters. Some cantons have jointly appointed an inter-cantonal data protection authority.
In the case of recommendations to private persons, the Commissioner may refer the case to the Swiss Federal Administrative Court for a decision. Both the Commissioner and the addressee of such a decision may file an appeal against the decision with the Swiss Federal Supreme Court.

The Commissioner does not have the power to issue any fines. However, based on Article 34 DPA, the competent criminal judge may, upon complaint, sanction private persons with a fine of up to 10,000 Swiss francs if they have wilfully breached their obligations to:

- provide information upon request of the data subject concerned under Article 8 DPA;
- provide information on the collection of sensitive personal data and personality profiles under Article 14 DPA;
- inform the Commissioner about the safeguards and data protection rules in relation to a transfer of personal data abroad under Article 6 Paragraph 3 DPA;
- register a database with the Commissioner; or
- cooperate with the Commissioner (Article 34 DPA).

Furthermore, anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to his or her knowledge in the course of his or her professional activities is, upon complaint, liable to a fine of up to 10,000 Swiss francs (Article 35 DPA in connection with Article 106 Paragraph 1 of the CC).

ii Recent enforcement cases

The Swiss Federal Supreme Court’s decision of 12 January 2015 in connection with the tax dispute between certain Swiss banks and the United States is particularly noteworthy. Based on the right of access set forth in Article 8 DPA, the Court obliged a Swiss bank to provide its employees with copies of all documents transferred to the US Department of Justice in April 2012 containing their personal data.

As regards the processing of employee personal data, the Swiss Federal Supreme Court held in 2013 that the monitoring of an employee’s use of email and internet that lasted for three months and included taking regular screenshots was illegal and not proportionate. Moreover, the monitoring was not backed by an internal policy that permitted monitoring under specific, transparently disclosed circumstances.

More recently, several court decisions have been rendered regarding data protection issues in connection with the granting of access to official documents based on the Swiss Federal Freedom of Information Act of 17 December 2004. In three parallel rulings dated 23 August 2016, the Swiss Federal Administrative Court decided on the scope of Article 19 Paragraph 4 Letter (a) and (b) DPA, according to which federal bodies shall refuse or restrict disclosure of documents, or make such disclosure subject to conditions if (1) essential public
interests or clearly legitimate interests of a data subject so require; or (2) statutory duties of confidentiality or special data protection regulations so require. In the case at hand, communal bodies requested access to documents from a closed bid-rigging proceeding investigated and decided by the Swiss Competition Commission in an attempt to collect evidence for civil follow-on actions. The Swiss Federal Administrative Court held that victims of anticompetitive conduct may be granted such access to information under the conditions that the information does not contain business secrets in the sense of Article 25 of the Swiss Federal Cartel Act of 6 October 1995 (ACart) and does not contain information provided by leniency applicants in the sense of Article 49a Paragraph 2 ACart.

On 11 May 2017, the Swiss Federal Administrative Court published a leading case dated 18 April 2017 relating to personality profiles and retrievability of personal data via search engines. The decision, which concerns a case of the Commissioner against a Swiss economic information platform and credit agency, is final and binding as none of the parties appealed against said decision. The Swiss Federal Administrative Court came to the conclusion that personal data that in combination reveals an essential part of the personality of a data subject and that is not relevant in assessing the creditworthiness of the person in question may not be published without the consent of the data subject concerned. The Commissioner’s claim that the economic information platform and credit agency’s data relating to persons registered in the commercial registry should only be retrievable with search engines in the same manner as data of the official Swiss Federal Commercial Registry was rejected (search engines, in particular Google, only show search results for the Swiss Commercial Registry (i.e., www.zefix.ch) if the search name and also the term ‘Zefix’ are entered into the search tool). The Swiss Federal Administrative Court stated that the economic information platform and credit agency only has limited influence on the publication of search results on search engines. Also, the Swiss Federal Administrative Court pointed out that the possibility of finding data via search engines may have positive effects from a data protection perspective as it increases transparency.

Lastly, the European Court of Human Rights (ECHR), in a ruling of 18 October 2016, overruled a decision of the Swiss Federal Supreme Court in the field of publicly regulated accident insurance. The Swiss Supreme Court had previously ruled that accident insurance companies could lawfully conduct secret surveillance of the candidates for, or beneficiaries of, insurance benefits, despite the absence of a sufficiently detailed legal basis. Subsequent to the ECHR ruling, the Swiss Federal Supreme Court, on 14 July 2017, in line with the ECHR ruling, decided that, likewise, the federal social security office could not lawfully conduct secret surveillance of candidates for or beneficiaries of disability insurance. The Swiss parliament is currently drafting an amendment that provides sufficient legal basis for such surveillance by specifically setting out applicable requirements and conditions.

### iii Private litigation

Any person may request information from the controller of a data file as to whether personal data concerning them is being processed (Article 8 Paragraph 1 DPA). This ‘right to information’ includes information about:

* the source of the personal data;

---

40 Classified compilation (SR) 251, last amended as of 1 December 2014.
the purpose of and, if applicable, the legal basis for, the processing as well as the
categories of the personal data processed;
the other parties involved in the processing; and
the data recipient concerned (Article 8 Paragraph 2 DPA).

This information must normally be provided in writing, in the form of a printout or
a photocopy, and is in principle free of charge (a fee of up to 300 Swiss francs may be levied
in exceptional cases outlined in Article 2 DPO). Any data subject may also request that
incorrect data be corrected (Article 5 Paragraph 2 DPA).

In addition, data subjects have ordinary judicial remedies available under civil law to
protect their personality rights (Article 15 DPA in relation to Article 28–28l of the Swiss
Civil Code). Data subjects may in particular request:
that data processing be stopped;
that no data be disclosed to third parties;
that the personal data be corrected or destroyed;
compensation for moral sufferings; and
payment of damages or the handing over of profits.

However, as regards claims for damages, it is in practice often very difficult for a data subject
to prove actual damage based on privacy infringements.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The territorial scope of application of the DPA is very broad. The DPA not only applies to
the processing of personal data in Switzerland (which is the most common trigger), but –
depending on the circumstances – may also apply to the processing of personal data that
takes place abroad. In fact, based on an international convention or based on Article 129
Paragraph 1 and Article 130 Paragraph 3 PILA, a data subject may in some instances have
the option to file an action in a Swiss court for infringement of his or her personality rights
and ask the competent court to apply Swiss law even if no processing activity has taken place
in Switzerland (cf. Article 139 PILA). Based on the foregoing, foreign organisations should
review compliance with the DPA even if they do not process any personal data in Switzerland
or even if they do not have any presence in Switzerland if there is a possibility that data
subjects may file a claim in Switzerland and ask for the application of the DPA.

As regards foreign organisations with personal data processing operations in
Switzerland (e.g., through a branch office, an affiliate or a third-party service provider),
compliance with the requirements on international data transfers is another important topic
if a cross-border exchange of personal data is involved (e.g., in the context of centralised HR
and customer relationship management systems – see Section IV). Moreover, if a foreign
organisation transfers or discloses personal data to Switzerland for the first time, additional
or new obligations for the processing of the personal data may be created that did not exist

42 This, however, does not apply to public law provisions of the DPA (such as the obligation to register a data
file with the Commissioner or to inform the Commissioner of a transfer abroad) as such rules are governed
by the principle of territoriality and only apply to facts that take place in Switzerland.
We therefore strongly recommend verifying compliance with the DPA before disclosing or transferring any personal data to Switzerland, before starting to process personal data in Switzerland (whether on one’s own or by using group companies or third-party service providers), or before cross-border exchanges of personal data in the context of a group of companies or otherwise.

IX  CYBERSECURITY AND DATA BREACHES

Article 7 DPA and Articles 8–12 DPO set out the general security requirements applicable to the processing of personal data. Additionally, the Commissioner has issued a guide pertaining to technical and organisational measures to be taken when processing personal data.44

Neither the DPA nor the DPO currently explicitly require data handlers to notify the Commissioner (nor any other Swiss authority) or data subjects of any suspected or actual personal data breaches (note that this is likely to change under the revised DPA).45 However, data handlers may indeed have a duty to inform data subjects concerned based on the principles of transparency and good faith. Data handlers may in certain circumstances also have a contractual obligation to notify data subjects of any suspected or actual personal data breaches.46 In the event that a large number of data subjects are affected, the principles of transparency and good faith may very exceptionally even result in a duty to report the incident publicly. This may in particular be the case if the data subjects concerned cannot be informed individually and there is a high probability that damages will occur if the incident is not publicly reported. Whether an obligation to notify data subjects exists (be it individually, through public reporting, or both) must be checked on a case-by-case basis.

In Switzerland, the cantons are generally responsible for the prosecution of misuse of information and communication technology. To fight cybercrime more efficiently, the Swiss Confederation and the cantons entered into an administrative agreement in 2001, empowering the federal authorities to assume certain responsibilities in this area. On 1 January 2014, the Swiss national coordination unit to fight internet crime, the Cybercrime

43 Such as, for example, an obligation to register a data file with the Commissioner, or there may be instances where data that before their transfer or disclosure to Switzerland were not subject to specific data protection regulations suddenly becoming subject to the data protection regulations set forth in the DPA and the DPO because of the fact that the DPA and DPO currently also apply to the processing of personal data pertaining to legal entities (even if, at a later stage, the data are transferred from Switzerland abroad again).

44 'Guide for technical and organisational measures' (status as of February 2016; www.edoeb.admin.ch/daten­schtutz/00628/00629/00636/index.html?lang=en, last visited on 27 September 2017). Additional security requirements apply to specific sectors such as, inter alia, the financial industry and the area of medical research. These additional requirements are set forth in separate legislative acts.

45 For certain specifically regulated areas, however, these duties may exist. This is the case, for instance, in the banking sector where regulatory requirements call for a notification in certain cases of data breaches (Circular 2008/21 – Operational Risks Banks, Annex 3, of the Swiss Financial Market Supervisory Authority – FINMA, available at: www.finma.ch/de/-/media/finma/dokumente/rundschreiben-archiv/finma-ts-2008-21---30-06-2017.pdf?sa=U&ved=0ahUKEwiZ8vteroovWAhUCshQKHcLuuBeMQFggNMAQ&client=interna­l-uds-cse&usg=AFQjCNH1i9Man6e87Na3Uq4hvV8R2iGy4g, last visited on 27 September 2017).

46 For example, a data handler may have an obligation to inform its customers about a data breach based on an explicit contractual obligation towards its customers or based on a general contractual duty of diligence.
Coordination Unit Switzerland (CYCO), commenced its activities. CYCO conducts an initial analysis of incoming reports, secures the relevant data and then forwards the matter to the competent law enforcement agencies in Switzerland and abroad.

On a Swiss federal level, the Reporting and Analysis Centre for Information Assurance (MELANI) was established in 2004. MELANI functions as a cooperation model, *inter alia*, between the Swiss Federal Finance Department and the Swiss Federal Defence Department. It serves private computers and internet users (in particular providing them with information about risks relating to the use of modern information and communication technologies) as well as selected providers of critical national infrastructures (such as banks and telecommunication services providers). MELANI has created various checklists and documentation regarding IT security. In 2008, MELANI established GovCERT.ch, the computer emergency response team (CERT) of the government, and the official national CERT of Switzerland, GovCERT.ch is a member of the Forum of Incident Response and Security Teams, and of the European Government CERTs group.


**X OUTLOOK**

The ongoing reform of the DPA is likely to lead to a tightening of the Swiss data protection regime. Based on the publication of the draft of the revised DPA, the following aspects are particularly noteworthy:

- **a** transparency in data processing is increased. In particular, private sector actors will have a duty to inform data subjects in the event of data collection and processing;
- **b** self-regulation shall be encouraged. Professional and business associations may prepare codes of conduct and submit them to the Commissioner for the delivery of an opinion;
- **c** the data controller will have to perform an impact assessment whenever it appears that the envisaged data processing may lead to an increased risk to the data subjects’ personality and fundamental rights, although some exceptions apply;
- **d** a duty to notify the Commissioner or even the data subjects in cases of breach of data protection will bind data controllers;
- **e** the present rules on personality profiles will be abolished. However, they will be replaced by new rules on profiling;
- **f** the draft introduces the concepts of privacy by design and privacy by default. Hence, data protection must take place from the outset (i.e., from the conception of the processing) and the least invasive settings must be applied by default;
- **g** the duty to declare data files to the Commissioner shall be abolished for private actors. Data controllers and data processors must, however, keep an inventory of their processing activities;

---


48 Classified compilation (SR) 351.1, status as of 1 January 2013.

49 See footnote 6 for links to the draft of the revised DPA.
personal data relating to legal entities will no longer be specifically protected under the DPA;
the Commissioner shall obtain greater powers and will in particular have the competence to render binding decisions on data controllers and processors; and
criminal sanctions for data protection misconduct will be increased significantly. In fact, fines of up to 250,000 Swiss francs may be levied in cases of intentional offences against certain provisions of the revised DPA.

Moreover, the revision process will affect not only the DPA itself, but also many other laws, such as the CC, criminal procedure regulations and so forth.

The text that will eventually become law, may contain deviations from the published draft. It is nonetheless to be expected that the final revised DPA will include many of the changes suggested in the draft of the revised DPA. Entry into force of the new, revised DPA is tentatively scheduled for 1 August 2018 at the earliest.
Chapter 26

UNITED KINGDOM

William RM Long, Géraldine Scali and Francesca Blythe

I OVERVIEW

Like other countries in Europe, the United Kingdom has adopted an omnibus data protection regime implementing the EU Data Protection Directive 95/46/EC (the Data Protection Directive), which regulates the collection and processing of personal data across all sectors of the economy. From 25 May 2018, the EU General Data Protection Regulation (the Regulation) will have direct effect in the United Kingdom and will repeal the Data Protection Directive. The government of the United Kingdom is also proposing a Data Protection Bill to implement the Regulation before it takes effect on 25 May 2018.

II THE YEAR IN REVIEW

On 21 June 2017 the Queen's Speech outlined the UK government’s legislative priorities for the next two years. This speech confirmed not only that the United Kingdom will still be an EU Member State when the Regulation takes effect, but also that the government intends to introduce legislation implementing the Regulation so that after Brexit, the United Kingdom will have a law on its books that implements the Regulation. A draft of this new Data Protection Bill was expected to be published in September 2017 and consultation documents, including the official Statement of Intent suggest that it will faithfully implement the Regulation. After Brexit, the UK government could of course amend this data protection law so that it diverges from the Regulation. However, were the government to do this, the wide extraterritorial scope of the Regulation means that many UK companies would still need to comply with the new requirements under the Regulation.

In the past months, the Information Commissioner’s Office (ICO) has begun to publish guidance in respect of the Regulation. In March 2017, the ICO published draft consent guidance for public consultation, and in April the ICO published a feedback request in relation to the profiling requirements under the Regulation. The ICO expects to publish

---

1 William RM Long is a partner, Géraldine Scali is a counsel and Francesca Blythe is an associate at Sidley Austin LLP.
3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
4 Department for Digital, Culture, Media and Sport, A new Data Protection Bill: Our Planned Reforms.
additional Regulation guidance before May 2018 and is currently considering whether to issue entirely new guidance documents or to adapt its existing guidance for the Regulation. On 29 November 2016, the Investigatory Powers Bill received royal assent and became known as the Investigatory Powers Act 2016 (IPA). The IPA, once brought fully into force, will reform the regime under which UK law enforcement bodies, intelligence agencies and the government can intercept communications, interfere with equipment and acquire and intercept bulk communications data.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

Until May 2018 (or until the date on which the proposed Data Protection Bill takes effect, if before 25 May 2018), data protection in the United Kingdom is mainly governed by the Data Protection Act 1998 (DPA), which implemented the Data Protection Directive into national law and entered into force on 1 March 2000.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulate direct marketing, but also the processing of location and traffic data and the use of cookies and similar technologies. The PECR have implemented Directive 2002/58/EC7 (as amended by Directive 2009/136/EC) (the ePrivacy Directive). On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace the existing ePrivacy Directive.8 The ePrivacy Regulation will complement the Regulation, have direct effect in Member States including the United Kingdom (unless the United Kingdom exits the European Union before the ePrivacy Regulation takes effect) and provide additional sector-specific rules including in relation to marketing and the use of website cookies.

The key changes in the proposed ePrivacy Regulation will:

a require a clear affirmative action to consent to cookies;
b attempt to encourage the shifting of the burden of obtaining consent for use of cookies to website browsers; and
c make consent for direct marketing harder to obtain and require it to meet the standard set out in the Regulation; however, existing exceptions (such as the exemption that applies where there is an existing relationship and similar products and services are being marketed) are likely to be retained.

The European Commission’s original timetable for the ePrivacy Regulation was for it to apply from 25 May 2018 and coincide with the Regulation. However, it is increasingly unlikely...
that this deadline will be met, both because the ePrivacy Regulation is tied to a wider reform of EU telecommunications regulation and also because of the number of issues with the proposal that have been identified.

In April 2017, the Article 29 Working Party issued an opinion on the proposed ePrivacy Regulation, which welcomed some elements of the proposal but also identified areas of ‘grave concern’, including with regard to cookie tracking walls.\(^9\) It is currently uncertain when the ePrivacy Regulation will be finalised and when it will take effect.

**Key definitions under the DPA**

\(a\) Data controller: a person 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;\(^10\)

\(b\) data processor: any person (other than the employee of a data controller) who processes the data on behalf of the data controller;\(^11\)

\(c\) data subject: an individual who is the subject of personal data;\(^12\)

\(d\) personal data: data that relate to a living individual who can be identified from that data, or from that data and other information that is in the possession of, or is likely to come into the possession of, the data controller;\(^13\)

\(e\) processing (in relation to information): obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data;\(^14\) and

\(f\) sensitive personal data: personal data consisting of information as to the racial or ethnic origin of the data subject, his or her political opinions, his or her religious beliefs, or information of a similar nature, whether the subject is a member of a trade union, his or her physical or mental health or condition, sexual life, the commission or alleged commission by him or her of any offence, or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.\(^15\)

**Data protection authority**

The DPA and PECR are enforced by the ICO and from 25 May 2017, the ICO will enforce the Regulation in the United Kingdom and any UK legislation implementing the Regulation. Once the ePrivacy Regulation is finalised and takes effect, the ICO will also enforce the

---


\(^10\) Section 1 DPA.

\(^11\) Ibid.

\(^12\) Ibid.

\(^13\) Ibid.

\(^14\) Ibid.

\(^15\) Section 2 DPA.
ePrivacy Regulation and any UK implementing legislation in the United Kingdom. The ICO also enforces and oversees the Freedom of Information Act 2000, which provides public access to information held by public authorities. The ICO has independent status and is responsible for:

a maintaining the public register of data controllers;
b promoting good practice by giving advice and guidance on data protection and working with organisations to improve the way they process data through audits, arranging advisory visits and data protection workshops;
c ruling on complaints; and
d taking regulatory actions.

ii General obligations for data handlers

Under the DPA, data controllers must comply with the eight data protection principles and ensuing obligations.

First principle: fair and lawful processing

Personal data must be processed fairly and lawfully. This essentially means that the data controller must:

a have a legitimate ground for processing the personal data;
b not use data in ways that have an unjustified adverse effect on the individuals concerned;
c be transparent about how the data controller intends to use the personal data, and give the data subject appropriate privacy notices when collecting their personal data;
d handle a data subject’s personal data only in ways they would reasonably expect and consistent with the purposes identified to the data subject; and
e make sure that nothing unlawful is done with the data.

Legal basis to process personal data

As part of fair and lawful processing, the processing must be justified by at least one of six specified grounds listed in Schedule 2 to the DPA.

The DPA applies a stricter regime in the case of sensitive personal data, which may only be processed on the basis of certain limited grounds, including where the data controller has obtained the explicit consent of the data subject.

Registration with the ICO

Under the DPA, a data controller processing personal data must make a notification to the ICO unless certain limited exemptions apply. A data controller who is not established in the United Kingdom, or any other European Economic Area (EEA) state, but is using equipment in the United Kingdom for processing personal data other than merely for the purposes of transit in the United Kingdom, has to appoint a representative in the United Kingdom and provide the contact name and details of the representative to the ICO in the registration.

---

16 Schedule 1 to the DPA.
17 See definition at Section III.i.
18 Schedule 3 to the DPA.
19 Section 18 DPA.
form. Notification of the ICO consists of filling in a form and the payment of a fee, which must be paid when the data controller registers for the first time and then every year when the registration is renewed.

**Data protection officer**

There is no current legal requirement to appoint a data protection officer.

**Information notices**

Data controllers must provide data subjects with information on how their personal data is being processed. In general terms, an information notice should, according to the ICO,\(^{20}\) state the data controller’s identity and, if the data controller is not based in the United Kingdom, the identity of its nominated UK representative; the purposes for which the processing of personal data is intended; and any additional information the data controller needs to give individuals in the circumstances to be able to process the data fairly.\(^ {21}\)

**Second principle: processing for specified and lawful purposes**

Personal data can only be obtained for one or more specified and lawful purposes, and must not be processed in a way that is incompatible with those purposes.

**Third principle: personal data must be adequate, relevant and not excessive**

A data controller must ensure that it holds sufficient personal data to fulfil its intended lawful purposes, but that personal data must be relevant and not excessive to those purposes.

**Fourth principle: personal data must be accurate and kept up to date**

Data controllers must ensure that personal data is accurate and, where necessary, kept up to date. The ICO recommends\(^ {22}\) data controllers take reasonable steps to ensure the accuracy of any personal data obtained, ensure that the source of any personal data is clear, and carefully consider any challenges to the accuracy of information and whether it is necessary to update the information.

**Fifth principle: personal data must not be kept for longer than necessary**

Personal data processed for particular purposes should not be kept for longer than is necessary for those purposes. In practice, this means that the data controller must review the length of time it keeps personal data and consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain this information. Data controllers must also securely delete personal data that is no longer needed for this purpose or these purposes, and update, archive or securely delete information if it goes out of date.

It is good practice to establish standard retention periods for different categories of information (e.g., employee data and customer data). To determine the retention period for each category of information, data controllers should take into account and consider any legal or regulatory requirements or professional rules that would apply.\(^ {23}\)

---


\(^{21}\) ICO, Guide to Data Protection, Part B1, Paragraph 25.

\(^{22}\) ICO, Guide to Data Protection.

\(^{23}\) Ibid.
Sixth principle: personal data must be processed in accordance with the rights of data subjects

Personal data should be processed in accordance with the rights of data subjects under the DPA. In particular, the data controller must:

a. provide information in response to a data subject’s access request; 24
b. comply with a justified request to prevent processing that is causing or will be likely to cause unwarranted damage or distress to the data subject or another person;
c. comply with a notice to prevent processing for the purposes of direct marketing; and
d. comply with a notice objecting to the taking of automated decisions.

Seventh principle: measures must be taken against unauthorised or unlawful processing of personal data

Appropriate technical and organisational measures must be taken by the data controller against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, the personal data. Where a data controller uses a data processor to process personal data on its behalf, then the data controller must ensure that it has entered into a written contract that obliges the data processor to process only the personal data on the instructions of the data controller and to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

Eighth principle: transfers of personal data to a country or territory outside the European Economic Area

See Section IV.

iii General obligations of data controllers and processors

For a summary of the general obligations of data controllers and processors under the Regulation, see Section III of the European Union Overview chapter.

iv Technological innovation and privacy law

Anonymisation

Neither the DPA nor the Regulation applies to anonymous data. However, there has been a lot of discussion over when data is anonymous and the methods that could be applied to anonymise data.

The ICO in its guidance on anonymisation 25 recommends organisations using anonymisation to have in place an effective and comprehensive governance structure that should include:

a. a senior information risk owner with the technical and legal understanding to manage the process;

b. staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them;

24 ICO, Subject Access Code of Practice, V.1.1, February 2014.
25 In November 2012, the ICO published a code of practice on managing data protection risks related to anonymisation. This code provides a framework for organisations considering using anonymisation and explains what it expects from organisations using such processes.
procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice;

d knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation;

e a joint approach with other organisations in the same sector or those doing similar work;

f use of a privacy impact assessment;

g clear information on the organisation’s approach to anonymisation, including how personal data is anonymised and the purpose of the anonymisation, the techniques used and whether the individual has a choice over the anonymisation of his or her personal data;

h a review of the consequences of the anonymisation programme; and

i a disaster-recovery procedure should re-identification take place and the individual’s privacy is compromised.

Big data

The DPA does not prohibit the use of big data and analytics. However, because it raises various data protection issues, the ICO issued guidance in July 2014 and revised it in August 2017 considering data protection issues raised by big data. The ICO suggests how data controllers can comply with the DPA and, from May 2018, the Regulation while using big data, covering a broad range of topics including anonymisation, privacy impact assessments, repurposing data, data minimisation, transparency and subject access. The guidance included three questions on which the ICO invited feedback. A summary of feedback on big data and data protection and the ICO position was published in April 2015.

In addition, the Financial Conduct Authority (FCA) published in March 2017 a feedback statement following its Call for Inputs on Big Data on retail general insurance. The FCA’s key findings were that although big data is producing a range of benefits for consumers in motor and home insurance, there are also concerns about its impact on data protection. To address some of these concerns the FCA proposed to co-host a roundtable with the ICO and various stakeholders to discuss data protection and the use of personal data in retail general insurance.

Bring your own device (BYOD)

The ICO has published guidance for companies on implementing BYOD programmes allowing employees to connect their own devices to company IT systems. Organisations using BYOD should have a clear BYOD policy so that employees connecting their devices to the company IT systems clearly understand their responsibilities.

To address the data protection and security breach risks linked to BYOD, the ICO recommends that companies take various measures, including:

a considering which type of corporate data can be processed on personal devices;

b how to encrypt and secure access to the corporate data;

c how the corporate data should be stored on the personal devices;

27 ICO, Summary of Feedback on Big Data and Data Protection and ICO Response, 10 April 2015.
28 FCA, FS16/5, Call for Inputs on Big Data in retail general insurance.
29 ICO, Guidelines on Bring Your Own Device (BYOD), 2013.
how and when the corporate data should be deleted from the personal devices; and

how the data should be transferred from the personal device to the company servers.

Organisations should also install antivirus software on personal devices, provide technical support to the employees on their personal devices when they are used for business purposes, and have in place a ‘BYOD acceptable-use policy’ providing guidance to users on how they can use their own devices to process corporate data and personal data.

Cloud computing

The use of cloud computing and how it complies with EU data protection requirements has been a subject of much discussion recently. The ICO, like many other data protection authorities in the EU, has published guidance on cloud computing.30

Cloud customers should choose their cloud provider based on economic, legal and technical considerations. According to the ICO, it is important that, at the very least, such contracts allow cloud customers to retain sufficient control over the data to fulfil their data protection obligations.

The ICO proposes a checklist that organisations can follow prior to entering into an agreement with a cloud provider, with questions on confidentiality, integrity, availability, and other legal and data protection issues.31

Cookies and similar technologies

In 2009, the e-Privacy Directive 2002/58/EC was amended.32 This included a change to Article 5(3) of the e-Privacy Directive requiring consent for the use of cookies and similar technologies. This new requirement was implemented in the United Kingdom through the PECR. As a result, organisations now have an obligation to obtain consent of website users to place cookies or similar technologies on their computers and mobile devices.33 The consent obligation does not apply where the cookie is used ‘for the sole purpose of carrying out the transmission of a communication over an electronic communication network’ or is ‘strictly necessary’ to provide the service explicitly requested by the user. This exemption is applied restrictively and so could not be used when using analytical cookies. Organisations must also provide users with clear and comprehensive information about the purposes for which the information, such as that collected through cookies, is used.

The ICO has published guidance on the use of cookies, and provides recommendations on how to comply with the requirements and how to obtain consent. The ICO considers that implied opt-in consent is a valid form of consent if the consenting individual has taken some action from which the consent can be inferred, such as visiting the website and going from one page to another by clicking on a particular button.34

31 See the European Union Overview chapter for more details on cloud computing.
32 Directive 2009/136/EC.
33 PECR Regulation 6.
On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace the existing ePrivacy Directive. The ePrivacy Regulation will complement the Regulation and provide additional sector-specific rules, including in relation to the use of website cookies.

v Specific regulatory areas

Employee data

There is no specific law regulating the processing of employee data. However, the ICO has published an employment practices code and supplementary guidance to help organisations comply with the DPA and to adopt good practice.

The code contains four parts covering:

a recruitment and selection, providing recommendations with regard to the recruitment process and pre-employment vetting;
b employment records, which is about collecting, storing, disclosing and deleting employees’ records;
c monitoring at work, which covers employers’ monitoring of employees’ use of telephones, internet, email systems and vehicles; and
d workers’ health, covering occupational health, medical testing and drug screening.

Employee monitoring

The DPA does not prevent employers monitoring their employees. However, monitoring employees will usually be intrusive, and workers have legitimate expectations that they can keep their personal lives private. Workers are also entitled to a degree of privacy in their work environment.

Organisations should carry out a privacy impact assessment before starting to monitor their employees to clearly identify the purposes of monitoring, the benefit it is likely to deliver, the potential adverse impact of the monitoring arrangement, and to judge if monitoring is justified, as well as take into account the obligation that arises from monitoring. Organisations should also inform workers who are subject to the monitoring of the nature, extent and reasons for monitoring unless covert monitoring is justified.

Employers should also establish a policy on use by employees of electronic communications, explaining acceptable use of internet, phones and mobile devices, and the purpose and extent of electronic monitoring. It should also be outlined how the policy is enforced and the penalties for a breach of the policy.

Opening personal emails should be avoided where possible and should only occur where the reason is sufficient to justify the degree of intrusion involved.

On 8 June 2017, the Article 29 Working Party adopted an opinion on data processing at work that also addressed employee monitoring. This opinion is unlikely to fundamentally change the ICO’s approach to employee monitoring in the United Kingdom. However,

36 See the European Union Overview chapter for more details on the proposed ePrivacy Regulation.
38 Ibid.
39 WP 249: Opinion 2/2017 on data processing at work, adopted 8 June 2017.
it does include a number of new recommendations, including that where it is possible to block websites rather than continually monitoring internet usage, employers should prefer prevention to detection.

**Whistle-blowing hotlines**

Under the DPA, the use of whistle-blowing hotlines (where employees and other individuals can report misconduct or wrongdoing) is permitted and their use is not restricted by the ICO. There is no specific UK guidance on the use of whistle-blowing hotlines. However, organisations using them in the United Kingdom will have to comply with the data-protection principles under the DPA and, from 25 May 2018, the Regulation.\(^{40}\)

**Electronic marketing\(^{41}\)**

Under the PECR, unsolicited electronic communication to individuals should only be sent with the recipient’s consent.\(^{42}\) The only exemption to this rule is known as ‘soft opt-in’, which will apply if the sender has obtained the individual’s details in the course of a sale or negotiations for a sale of a product or service; the messages are only marketing for similar products; and the person is given a simple opportunity to refuse marketing when his or her details are collected, and if he or she does not opt out, he or she is given a simple way to do so in future messages. These UK rules on consent do not apply to marketing emails sent to companies and other corporate bodies.\(^{43}\)

Senders of electronic marketing messages must provide the recipients with the sender’s name and a valid contact address.\(^{44}\)

The ICO has created a direct-marketing checklist, which enables organisations to check if their marketing messages comply with the law and which also proposes a guide to the different rules on marketing calls, texts, emails, faxes and mail. The ICO has also published guidance on direct marketing, which it updated in March 2016.\(^{45}\)

The proposed ePrivacy Regulation, which will have direct effect in the United Kingdom if it takes effect before the United Kingdom exits the European Union, will supersede the PECR. The current draft of the ePrivacy Regulation would require a higher standard of consent for direct marketing, equivalent to the consent standard in the Regulation. However, it is possible that existing exemptions such as the soft opt-in may be retained.\(^{46}\)

---

\(^{40}\) For guidance on how to comply with data protection principles under the DPA see WP 117: Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime adopted on 1 February 2006.

\(^{41}\) ICO, Guide to the Privacy and Electronic Communications Regulations, 2013, and Direct Marketing Guidance, V.2.2.

\(^{42}\) PECR Regulation 22(2).

\(^{43}\) ICO, Direct Marketing Guidance, V.2.2.

\(^{44}\) PECR Regulation 23.

\(^{45}\) ICO, Direct Marketing Guidance, V.2.2.

\(^{46}\) See the European Union overview chapter for more details on the proposed ePrivacy Regulation.
**Financial services**

Financial services organisations, in addition to data protection requirements under the DPA, also have legal and regulatory responsibilities to safeguard consumer data under the rules of the FCA, which include having adequate systems and controls in place to discharge their responsibilities.

This includes financial services firms taking reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime, such as by misuse of customer data.\(^{47}\)

Failure to comply with these security requirements may lead to the imposition of significant financial penalties by the FCA.

**IV INTERNATIONAL DATA TRANSFER**

Under the eighth principle of the DPA, and under Article 45 of the Regulation, personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.\(^{48}\) The DPA and the Regulation provide various exemptions to permit transfers of personal data from the EEA to countries outside the EEA that do not provide an adequate level of protection, including:

\(a\) Consent: with the consent of the data subject, although as the ICO comments, valid consent means the data subject must have a real opportunity to withhold consent without incurring a penalty, or to subsequently withdraw consent. As a result, consent is unlikely to provide an adequate long-term framework in cases of repeated or structured transfer.

\(b\) EU–US Privacy Shield: US companies that self-certify under the Privacy Shield will be able to receive personal data from the EU in compliance with EU data protection requirements. The Privacy Shield was adopted on 12 July 2016 and replaces the US–EU Safe Harbor framework, which was invalidated by the CJEU in October 2015, in the iconic Schrems decision.\(^{49}\) US companies have been able to self-certify their compliance to the Privacy Shield Principles since 1 August 2016.

\(c\) EU Model Contract Clauses: where the EU’s standard contractual clauses (model contracts) for the transfer of personal data from a data exporter in the EEA to a data importer outside the EEA are entered into.

\(d\) Binding corporate rules: where the data controller has entered into binding corporate rules. As the lead data protection authority, the ICO has approved the binding corporate rules of 31 organisations so far.\(^{50}\)

\(e\) Adequacy assessment: where in the view of the data controller there is an adequate level of protection for the personal data to be transferred. This requires an assessment of the circumstances of the transfer (such as the nature of the data, the purposes of the transfer, security measures taken, etc.) and an assessment of the law in force in the country where the data is to be transferred.

---

47 SYSC 3.
48 Schedule 1 to the DPA, and Article 45 of the Regulation.
49 Case C-362/14 Schrems v. Data Protection Commissioner [2014].
50 To find the list of authorised binding corporate rules by the ICO see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.
Other exceptions under the DPA and the Regulation are:

- where it is necessary for carrying out certain types of contract or if the transfer is necessary to set up the contract;
- where it is necessary for reasons of substantial public interest (e.g., preventing and detecting crime, national security and collecting tax);
- where it is necessary for the protection of the vital interests of the individual (e.g., matters of life and death);
- where the personal data is part of a public register, as long as the person to whom the data is transferred complies with any restrictions on access to, or use of, the information in the register; and
- where it is necessary in connection with legal proceedings (including future proceedings not yet under way), to get legal advice or where exercising or defending legal rights.

V DISCOVERY AND DISCLOSURE

The ICO has not published any specific guidance on this topic.\(^{51}\) E-discovery procedures and the disclosure of information to foreign enforcement agencies will, most of the time, involve the processing of personal data. As a result, organisations will have to comply with the data protection principles under the DPA in relation to e-discovery and from 25 May 2018 must comply with the requirements of the Regulation.

In practice, this will mean informing data subjects about the processing of their personal data for this purpose. Organisations will also have to have a legal basis for processing the data. In the United Kingdom, companies may be able to rely on the legitimate-interest basis to disclose personal data unless the data contain sensitive data, in which case consent of the data subject will have to be obtained, or where the processing is necessary for the purposes of establishing, exercising or defending legal rights.\(^{52}\)

A data transfer solution will also have to be implemented if the data is sent to a country outside the EEA that is not deemed to provide an adequate level of protection as discussed in Section IV.

VI PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The ICO is responsible for enforcing the DPA. In the event of a breach the ICO may:

- issue information notices requiring organisations to provide the ICO with specified information within a certain period;
- issue undertakings committing an organisation to a particular course of action to improve its compliance;
- issue enforcement notices and ‘stop now’ orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law;

\(^{51}\) The Article 29 Working Party has, however, published a working document on this topic. See the European Union Overview chapter for more details.

\(^{52}\) Schedule 3(6)(c) to the DPA.
conduct consensual assessments (audits) to check organisations are complying. In the past, the ICO’s audit activities have been limited to assessments carried out with the consent of the organisations concerned. Now, however, the ICO may also issue an ‘assessment notice’, which enables it to inspect a government department or an organisation of a designated description to see whether it is complying with the data protection principles. The ICO does not need the organisation’s consent to do this if it has issued the notice;

issue assessment notices to conduct compulsory audits to assess whether organisations processing personal data follow good practice (data protection only);

issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010, or serious breaches of the PECR occurring on or after 26 May 2011;

prosecute those who commit criminal offences under the DPA. The ICO liaises with the Crown Prosecution Service to bring criminal prosecutions against organisations and individuals for breaches of the DPA; and

report to Parliament on data protection issues of concern.

The FCA also has enforcement powers and can impose financial penalties on financial services organisations for failure to comply with their obligations to protect customer data.

From 25 May 2018, the ICO will be responsible for enforcing the Regulation in the United Kingdom. In the event of a breach of the Regulation, the ICO may take the same actions as are available to it under the DPA, with the exception that the ICO will be able to issue monetary penalty notices of up to €20 million (or £17 million as proposed in the Data Protection Bill) or 4 per cent of annual worldwide turnover, whichever is greater.

**Recent ICO-led enforcement cases**

In May 2016, an NHS trust was issued with a £185,000 monetary penalty notice for publishing an equality and diversity spreadsheet on its website that contained confidential and sensitive personal data relating to a large number of employees and that was available to and accessible by the public for a number of months.

In August 2016, a GP surgery was issued with a £40,000 monetary penalty notice for releasing confidential information about a woman and her family to her estranged ex-partner.

In August 2016, a county council was issued with a £100,000 monetary penalty notice for leaving in an unlocked cupboard files containing confidential and sensitive personal data about 100 of its social care clients.

In October 2016, a telecom company was fined a record amount of £400,000 by the ICO for security failings that allowed an attacker to access large volumes of customers’ personal data.

In January 2017, the ICO fined an insurance company £150,000 following the loss of the personal data of nearly 60,000 customers.

In July 2017, an NHS trust was issued with a request to sign an undertaking in respect of its failure to comply with the DPA when sharing patient details with an AI system.

In August 2017, the ICO issued a telecom company with a monetary penalty notice of £100,000 after it failed to protect the personal data of up to 21,000 customers.

---

53 For central government organisations.
VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA applies to a data controller established in the United Kingdom and processing personal data in the context of that establishment. It also applies to foreign organisations not established in the United Kingdom, or in any other EEA state, that use equipment located in the United Kingdom (e.g., a service provider processing personal data in the United Kingdom) for processing personal data otherwise than for the purposes of transit through the United Kingdom. Data controllers not established in the United Kingdom or any other EEA country and processing personal data through equipment located in the United Kingdom must nominate a representative established in the United Kingdom and comply with the data principles and requirements under the DPA.

The Regulation will apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EEA, regardless of whether or not the processing takes place in the EEA. The Regulation will also apply to controllers or processors not established in the EEA that process the personal data of data subjects in the EEA in relation to the offering of goods and services to those data subjects in the EEA and to the monitoring of the behaviour of those data subjects in the EEA. Data controllers not established in the EEA but still subject to the Regulation nominate a representative established in one of Member States of the EEA.

VIII CYBERSECURITY AND DATA BREACHES

i Cybersecurity


The Investigatory Powers Act received Royal Assent on 29 November 2016. The Act prohibits the interception of communications without lawful authority and sets out the situations in which there is lawful authority. Various law enforcement and intelligence authorities can, under the Investigatory Powers Act, make targeted demands on telecommunications operators.

Under the Investigatory Powers Act, the Secretary of State may by giving notice require a public telecommunications operator to retain communications data for a period that must not exceed 12 months if he or she considers that this is necessary and proportionate for one or more of the purposes for which communications may be obtained under the Investigatory Powers Act. The Investigatory Powers Act also expands the data retention requirements in the DRIP Act that it replaces (see below) to a broader range of communications data, such as site browsing histories.

The Investigatory Powers Act is controversial and like its predecessor, the DRIP Act, it has been criticised for lacking basic safeguards and for granting overly expansive powers for the bulk collection of data. The legality of the Investigatory Powers Act has already been called into question following a ruling of the CJEU on the data retention provisions in the DRIP Act. One year after receiving Royal Assent, the English High Court issued a landmark judgment declaring the DRIP Act unlawful. The High Court ruled that a number of the provisions in the DRIP Act were incompatible with EU human rights law. However, the ruling was suspended until 31 March 2016 to give UK legislators time to implement appropriate safeguards. Preliminary questions were referred to the CJEU by the English Court of Appeal. On 21 December 2016, the CJEU issued a landmark ruling that effectively upheld an original decision of the High Court in relation to the validity of the provisions of
the DRIP Act.\textsuperscript{54} Although the ruling concerned the DRIP Act, the Investigatory Powers Act does little to address the criticisms of the DRIP Act in the CJEU’s judgment and in some cases provides for even more extensive powers than under the DRIP Act. The case has now been returned to the Court of Appeal, which initially referred questions to the CJEU for a preliminary ruling. As of August 2017, the Court of Appeal had not issued its judgment, but it is possible that one potential consequence of the judgment, once eventually received, is that the Investigatory Powers Act will need to be amended, either by further primary legislation or a statutory instrument.


The interception powers in Part 1, Chapter 1 of RIPA have been repealed and replaced by a new targeted interception power under the Investigatory Powers Act.

The DRIP Act

The DRIP Act has now been repealed and replaced by the Investigatory Powers Act. The DRIP Act was an emergency piece of legislation, and was due to expire on 31 December 2016.

UK cybersecurity strategy

In November 2011, the Cabinet Office published the UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, with four objectives for the government to achieve by 2015:

\begin{itemize}
  \item[a] tackling cybercrime and making the United Kingdom one of the most secure places in the world to do business;
  \item[b] to be more resilient to cyberattacks and better able to protect our interests in cyberspace;
  \item[c] to create an open, stable and vibrant cyberspace that the UK public can use safely and that supports open societies; and
  \item[d] to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives.
\end{itemize}

In March 2013, the government launched the Cyber-security Information Sharing Partnership to facilitate the sharing of intelligence and information on cybersecurity threats between the government and industry.

The government has also recently developed the Cyber Essentials scheme, which aims to provide clarity on good cybersecurity practice.

Along with the Cyber Essentials scheme, the government has published the Assurance Framework, which enables organisations to obtain certifications to reassure customers, investors, insurers and others that they have taken the appropriate cybersecurity precautions. The voluntary scheme is currently open and available to all types of organisation.

In June 2015, the government launched a new online cybersecurity training course to help the procurement profession stay safe online.

In July 2015, the government announced the launch of a new voucher scheme to protect small businesses from cyberattacks, which will offer micro, small and medium-sized businesses up to £5,000 for specialist advice to boost their cybersecurity and protect new business ideas and intellectual property.

\textsuperscript{54} Case C-698/15 Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis.
In January 2016, the government announced plans to assist start-ups offering cybersecurity solutions. Such start-ups will be given help, advice and support through the Early State Accelerator Programme, a £250,000 programme designed to assist start-ups in developing their products and bringing them to market. The programme is run by Cyber London and the Centre for Secure Information Technologies, and is funded by the government’s National Cyber Security Strategy programme.

In March 2016, the government announced that the United Kingdom’s new national cyber centre (announced in November 2015) would be called the National Cyber Security Centre (NCSC). The NCSC, which is based in London, opened in October 2016 and is intended to help tackle cybercrime.

**Data breaches**

Under the DPA, there is no requirement to report security breaches to the ICO and the individuals involved. Although there is no legal obligation on data controllers to report security breaches, the ICO believes that serious breaches should be brought to its attention. According to the ICO, there should be a presumption to report a breach to the ICO if a significant volume of personal data is concerned and also where smaller amounts of personal data are involved but there is still a significant risk of individuals suffering substantial harm. The ICO has issued varied guidance on how to manage security breaches and how to make a security-breach notification. In addition, under the PECR and the Notification Regulation, internet and telecommunication service providers must report breaches to the ICO no later than 24 hours after the detection of a personal data breach where feasible. The ICO has published guidance on this specific obligation to report breaches.

From 25 May 2018, under the Regulation there will be a requirement for data controllers to report personal data breaches to the ICO without undue delay and, where feasible, no later than 72 hours after the controller becomes aware of the breach. If a controller does not report the data breach within 72 hours, it must provide a reasoned justification for the delay in notifying the ICO. The controller is also subject to a concurrent obligation to notify affected data subjects without undue delay when the notification is likely to result in a high risk to the rights and freedoms of natural persons. Under the Regulation, data processors also have an obligation to notify the data controller of personal data breaches without undue

---

57 PECR Regulation 5A(2).
59 Article 2 of the Notification Regulation. The content of the notification is detailed in Annex 1 to the Notification Regulation.
60 ICO, Guidance on Notification of PECR Security Breaches, 26 September 2013.
61 Article 33(1) of the Regulation.
62 Article 34 of the Regulation.
delay after becoming aware of a personal data breach. According to its programme of work for 2017, the Article 29 Working Party is expected to produce guidelines on the notification of personal data breaches later in 2017.

IX OUTLOOK

The Regulation will apply in Member States from 25 May 2018. How long it will remain directly applicable in the United Kingdom will depend on how quickly the United Kingdom exits the European Union, and on the nature and content of any transitional agreement. The Queen's Speech in June 2017 confirmed that the United Kingdom will still be an EU Member State when the Regulation takes effect and that the government intends to introduce legislation implementing the Regulation. After Brexit, it is therefore likely that the United Kingdom will have passed a law, the proposed Data Protection Bill, that implements the Regulation. A draft of this new Data Protection Bill was expected to be published in September 2017. After Brexit, the UK government would be free to amend this data protection law so that it diverges from the Regulation; however, the government has not indicated an intention to do so. Instead, the UK government has published a position paper that proposes a close and ambitious model for UK–EU data protection cooperation after Brexit that will provide for ‘continued regulatory cooperation between the UK and EU data protection regulators and promote certainty for business, public authorities and citizens’.

The ICO has indicated that it intends to develop its Overview of the General Data Protection Regulation into a more detailed Guide to the General Data Protection Regulation, which will form the core of its guidance in respect of the Regulation. In addition, the ICO is scheduled to finalise its guidance on consent under the Regulation before the end of 2017 and to produce draft guidance on contracts and liability under the Regulation.

In the coming months, it is also likely to become clearer how the United Kingdom will implement the Network and Information Systems Directive (the NIS Directive). The NIS Directive was adopted in June 2016 by the European Parliament and, among other things, introduces stringent new information security requirements for ‘operators of essential services’ and ‘digital service providers’. Member States have until 9 May 2018 to implement the NIS Directive. The UK government confirmed that the NIS Directive would be implemented in the United Kingdom in a report published in December 2016. In August 2017, the government published a consultation on its plans to transpose the NIS Directive. The consultation closed on 30 September 2017 and, importantly, it considered the essential services that the NIS Directive should cover.

63 Article 33(2) of the Regulation.
I OVERVIEW

Although not universally acknowledged, the US commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The US privacy system has a relatively flexible and non-prescriptive nature, relying more on post hoc government enforcement and private litigation, and on the corresponding deterrent value of such enforcement and litigation, than on detailed prohibitions and rules. With certain notable exceptions, the US system does not apply a ‘precautionary principle’ to protect privacy, but rather allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin a party from, ‘unfair or deceptive’ business practices. However, US federal law does impose affirmative prohibitions and restrictions in certain commercial sectors, such as those involving financial and medical data, and electronic communications, as well as with respect to children’s privacy, background investigations and ‘consumer reports’ for credit or employment purposes, and certain other specific areas. State laws add numerous additional privacy requirements.

Legal protection of privacy in civil society has been recognised in US common law since 1890, when the article ‘The Right to Privacy’ was published in the Harvard Law Review by Professors Samuel D Warren and Louis D Brandeis. Moreover, from its conception by Warren and Brandeis, the US system for protecting privacy in the commercial realm has been focused on addressing technological innovation. The Harvard professors astutely noted that ‘[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […] the right “to be let alone”’. In 1974, Congress enacted the federal Privacy Act, regulating government databases, and found that ‘the right to privacy is a personal and fundamental right protected by the Constitution of the United States’. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices that have been incorporated in many other data protection regimes, including the European Union’s 1995 Data Protection Directive.

1 Alan Charles Raul is a partner and Frances E Faircloth is an associate at Sidley Austin LLP. Vivek K Mohan was previously an associate at Sidley and is now senior privacy and cybersecurity counsel at Apple Inc. His contribution to this chapter predated his work at Apple. The authors wish to thank Tasha D Manoranjan, an associate at Sidley Austin LLP, for her contribution to a prior version of this chapter. Passages of this chapter were originally published in ‘Privacy and data protection in the United States’, The debate on privacy and security over the network: Regulation and markets, 2012, Fundación Telefónica; and Raul and Mohan, ‘The Strength of the U.S. Commercial Privacy Regime’, 31 March 2014, a memorandum to the Big Data Study Group, US Office of Science and Technology Policy.
The United States has also led the way for the world not only in establishing model legal data protection standards in the 1974 Privacy Act, but also in terms of imposing affirmative data breach notification and information security requirements on private entities that collect or process personal data from consumers, employees and other individuals. The state of California was the path-breaker on data security and data breach notifications by first requiring in 2003 that companies notify individuals whose personal information was compromised or improperly acquired. Since then, approximately 48 states,² the District of Columbia and other US jurisdictions, and the federal banking, healthcare and communications agencies, have also required companies to provide mandatory data breach notifications to affected individuals, and have imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information. Dozens of other medical and financial privacy laws also exist in various states. There is, however, no single omnibus federal privacy law in the United States. Moreover, there is no designated central data protection authority in the United States, although the Federal Trade Commission (FTC) has primarily assumed that role for consumer privacy. The FTC is independent of the President, and is not obliged (although it is encouraged) to respect the Administration’s perspective on the proper balance between costs and benefits with respect to protecting data privacy. The Chair of the FTC is designated by the President, however, and may be removed as Chair (although not as one of the FTC’s five commissioners) at the discretion of the President.

As in the EU and elsewhere, privacy and data protection are balanced in the United States in accordance with other rights and interests that societies need to prosper and flourish, namely economic growth and efficiency, technological innovation, property and free speech rights and, of course, the values of promoting human dignity and personal autonomy. The most significant factor in counterbalancing privacy protections in the United States, perhaps, is the right to freedom of expression guaranteed by the First Amendment. Preserving free speech rights for everyone certainly entails complications for a ‘right to be forgotten’, since one person’s desire for oblivion may run counter to another’s sense of nostalgia (or some other desire to memorialise the past for good or ill).

The First Amendment has also been interpreted to protect people’s right to know information of public concern or interest, even if it trenches to some extent on individual privacy. Companies have also been deemed to have a First Amendment right to communicate relatively freely with their customers by exchanging information in both directions (subject to the information being truthful, not misleading and otherwise not the subject of an unfair or deceptive business practice).

The dynamic and robust system of privacy governance in the United States marshals the combined focus and enforcement muscle of the FTC, state attorneys general, the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services, the Department of Education, the judicial system, and last – but certainly not least – the highly motivated and aggressive US private plaintiffs’ bar. Taken together, this enforcement ecosystem has proven to be nimble, flexible and effective in adapting to rapidly changing technological developments and practices,

² New Mexico enacted its data breach notification law in 2017. Alabama passed data breach notification legislation in the Senate in April 2016, but companion legislation still has not made it through the Alabama House. If enacted, Alabama will become the 49th state to adopt a breach notification law. Alabama and South Dakota remain the only states without legislation specifically requiring data breach notification.
responding to evolving consumer and citizen expectations, and serving as a meaningful agent of deterrence and accountability. Indeed, the US enforcement and litigation-based approach appears to be particularly well suited to deal with ‘recent inventions and business methods’ – namely new technologies and modes of commerce – that pose ever-changing opportunities and unpredictable privacy challenges.

II THE YEAR IN REVIEW

Privacy and cybersecurity remain hot topics for regulators, and the past year has seen a number of agencies that previously exercised a limited mandate in this area issue guidance and pursue enforcement actions. The courts have also been active, and a number of recent cases promise to reshape the legal landscape for years to come.

As detailed below, the FTC has continued to play a leading role at the federal level on these issues. Other government agencies announced their focus on these issues, often issuing guidance for entities that fall within their regulatory sphere of influence. The SEC has exercised increasingly aggressive oversight regarding cybersecurity compliance and practices of broker-dealers and investment advisers. It announced exam priorities, and brought an enforcement action against an investment adviser that failed to maintain cybersecurity policies and procedures. The Department of Justice has also issued guidance for addressing data breach incidents, and for interacting with federal law enforcement. The FCC has remained interested in robocalls, imposing a fine against Travel Club for nearly US$3 million in 2015 for violating the FCC’s robocall rules by robocalling over 100 consumers without their consent. Many of the consumers had registered on the national ‘do not call’ registry. The case evidences the FCC’s increased focus on preventing robocalls.

In March 2017, Congress rejected FCC regulations first proposed in December 2016 from taking effect. The regulations would have subjected internet service providers (ISPs) to the authority of the FCC and would have imposed significant constraints on ISPs’ ability to use data they collect from their customers – without imposing comparable restrictions on other internet players. While the congressional action rescinded the FCC’s privacy rules for ISPs, it left FCC jurisdiction in place. In this context, FCC jurisdiction essentially precludes the FTC from regulating ISPs. Acting FTC Chairman Maureen Ohlhausen and newly appointed FCC Chairman Ajit Pai issued a joint statement agreeing that jurisdiction over broadband providers’ privacy and data security practices should be returned to the FTC, but until that occurs, the agencies will strive to harmonise the FCC privacy rules for broadband providers with the FTC standards for other companies.

States have continued to push privacy and cybersecurity initiatives forward. New Mexico became the 48th state to enact a data breach notification law, leaving Alabama and South Dakota as the only states that do not have a data breach notification requirement. The New Mexico law requires notice within 45 days of the discovery of a breach, although notice is not required where there is no significant risk of identity theft. Delaware and Virginia have updated their breach notification laws. Delaware added requirements for companies to ‘implement and maintain reasonable security’; provide identity theft protection to consumers whose social security numbers are affected; and notify the state attorney general if more than 500 residents are affected. Virginia now requires companies to notify the state attorney general if the breach involves tax information or affects more than 1,000 residents.

On 16 May 2017, Washington became the third state to pass a law regulating biometric data, which governs the collection, use and retention of ‘biometric identifiers’, including
fingerprints, voice prints, eye retinas, irises, or other patterns or characteristics that can be used to identify someone. The law specifically excludes ‘physical or digital photograph, video or audio recording or data generated therefrom’ (in addition to certain health-related data), suggesting the statute will have limited application in the context of facial-recognition technology. The law restricts the sale, lease and other disclosure of the data and requires its protection, but like a similar law in Texas, it does not provide for a private right of action. Illinois, the other state to pass a biometric data law, does, however, provide for a private cause of action, which has already spawned some litigation. Other states, including Connecticut, New Hampshire and Alaska, are considering the regulation of biometric data.

One case that saw continued development in early 2017 was *Spokeo, Inc v. Robins*. Thomas Robins had sued Spokeo for wilful violations of the Fair Credit Reporting Act (FCRA), alleging that inaccurate information disclosed about him on Spokeo’s website harmed his employment opportunities. In May 2016, the Supreme Court remanded the case to the Ninth Circuit for consideration of whether Robins had suffered an injury that was sufficiently ‘concrete’ to find standing. On remand from the Supreme Court, on 15 August 2017, the Ninth Circuit held that an alleged injury was sufficiently ‘concrete’, citing the harms that may arise when persons’ personal information is misused or improperly accessed.

In data breach litigation, courts continue to disagree about whether plaintiffs should prevail where they cannot allege that the criminal actually misused stolen data. In August 2017, the DC Circuit held that plaintiffs making allegations related to a 2015 breach had plausibly alleged a risk of harm, even without proving that their potentially stolen social security numbers had already been misused. Meanwhile, the Eighth Circuit held – on the one hand – that a plaintiff had standing to sue a company after a breach based on the theory that the plaintiff had paid for a certain level of security, and thus, the plaintiff arguably did not get the value of that bargain. On the other hand, however, the same court held that the case should be dismissed for failure to state a claim because of lack of evidence that anyone actually suffered fraud or identity theft resulting in financial loss. Moreover, the court stated that: ‘[t]he implied premise that because data was hacked [the company’s] protections must have been inadequate is a “naked assertion devoid of further factual enhancement” that cannot survive a motion to dismiss’ and ‘massive class action litigation should be based on more than allegations of worry and inconvenience’.

Amid this uncertainty, large-scale breaches and attacks continue to occur. On 12 May 2017, the WannaCry attack disabled computers in organisations across the world, including the UK National Health Service. Hackers, believed to be in North Korea, demanded money to unfreeze the computers. WannaCry exploited weaknesses in unpatched Windows XP operating systems and wreaked havoc in the United States, the United Kingdom and around the world. On 7 September 2017, Equifax, one of the three major consumer credit reporting agencies, announced that it had suffered a hack that potentially compromised the data of 143 million Americans.

### FTC actions

In October 2016, the FTC announced the release of a new guide for businesses dealing with data breaches. The guide covers the process businesses should follow and what officials they should contact when there is a data breach. It includes advice regarding secure systems, managing service providers, segmenting networks and notifying users whose information has been stolen. The FTC also released a video explaining much of the same material.
On 6 February 2017, the FTC announced that VIZIO had agreed to pay $2.2 million to settle charges by the FTC and the New Jersey attorney general that it installed software on TVs to collect viewing data of its 11 million customers without their knowledge or consent. The order required VIZIO to prominently disclose and obtain affirmative express consent for data collection and sharing. The settlement also required VIZIO to delete all data it collected before 1 March 2016 and to implement a comprehensive data privacy programme that would be regularly assessed.

On 15 August 2017, the FTC reached a settlement with Uber regarding allegations that the company had misrepresented its cybersecurity protections and engaged in unreasonable cybersecurity practices. The settlement sheds greater light on what the FTC means by the ‘reasonable data security’ measures it expects companies to take. Uber suffered a breach of its drivers’ location and other data and was the subject of 2014 news reports that alleged Uber employees could gain access to and use its customers’ personal information, including precise geolocation data. The FTC settlement clarified the core elements of a ‘reasonable’ data security programme, including restricted employee access to sensitive data, multi-factor authentication for remote access and encryption of sensitive personal data both in transit and at rest. The Court of Justice of the European Union (CJEU) has had an outsize impact on privacy and data protection issues that affect US companies. The CJEU decision invalidating the US–EU Safe Harbor in October 2015 led to lengthy negotiations between US and EU authorities on an appropriate replacement mechanism for data transfers across the Atlantic, resulting in the EU–US Privacy Shield Framework (Privacy Shield), which has been in place for more than a year. The FTC has brought three recent enforcement actions alleging that companies made false claims about Privacy Shield participation. In all three complaints, the FTC alleged the companies falsely stated in their privacy policies that they would comply with Privacy Shield, because the companies started the application for Privacy Shield compliance but did not complete the necessary steps to ensure full compliance before claiming they were Privacy Shield participants.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The United States has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk:

a financial, insurance and medical information;
b information about children and students;
c telephone, internet and other electronic communications and records;
d credit and consumer reports and background investigations at the federal level; and
e a further extensive array of specific privacy laws at the state level.

Moreover, the United States is the unquestioned world leader in mandating information security and data breach notifications, without which information privacy is not possible. If one of the sector-specific federal or state laws does not cover a particular category of data or information practice, then the Federal Trade Commission Act (FTCA), and each state’s ‘little FTCA’ analogue, comes into play. Those general consumer protection statutes broadly, flexibly and comprehensively proscribe (and authorise tough enforcement against) unfair or deceptive acts or practices. The FTC is the de facto privacy regulator in the United States. State attorneys general and private plaintiffs can also enforce privacy standards under analogous
‘unfair and deceptive acts and practices’ standards in state law. Additionally, information privacy is further protected by a network of common law torts, including invasion of privacy, public disclosure of private facts, ‘false light’, appropriation or infringement of the right of publicity or personal likeness, and, of course, remedies against general misappropriation or negligence. In short, there are no substantial lacunae in the regulation of commercial data privacy in the United States. In taking both a general (unfair or deceptive) and sectoral approach to commercial privacy governance, the United States has empowered government agencies to oversee data privacy where the categories and uses of data could injure individuals.

**FTCA**

Section 5 of the FTCA prohibits ‘unfair or deceptive acts or practices in or affecting commerce’. While the FTCA does not expressly address privacy or information security, the FTC applies Section 5 to information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities. The FTC has brought successful enforcement actions under Section 5 against companies that failed to adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments or failed to provide a ‘fair’ level of security for consumer information.

Under Section 5, an act or practice is deceptive if there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and the representation or omission is ‘material’ – defined as an act or practice ‘likely to affect the consumer’s conduct or decision with regard to a product or service’. An act or practice is ‘unfair’ under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition.

The FTC takes the position that companies must disclose their privacy practices adequately, and that in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses. The FTC brought an enforcement action in 2009 against Sears for allegedly failing to adequately disclose the extent to which it collected personal information by tracking the online browsing of consumers who downloaded certain software. The consumer information allegedly collected included ‘nearly all of the Internet behavior that occurs on [. . .] computers’. The FTC required Sears to prominently disclose any data practices that would have significant unexpected implications in a separate screen outside any user agreement, privacy policy or terms of use.

Section 5 is also generally understood to prohibit a company from using previously collected personal data in ways that are materially different from, and less protective than, what it initially disclosed to the data subject, without first obtaining the individual’s additional consent.

The FTC staff has also issued extensive guidance on online behavioural advertising, emphasising four principles to protect consumer privacy interests:

- **a** transparency and control, giving meaningful disclosure to consumers, and offering consumers choice about information collection;
- **b** maintaining data security and limiting data retention;
express consent before using information in a manner that is materially different from the privacy policy in place when the data were collected; and

d express consent before using sensitive data for behavioural advertising.

The FTC’s report does not, however, require opt-in consent for the use of non-sensitive information in behavioural advertising.

**Fair information practice principles**

The innovative American privacy doctrine elaborated theories for tort and injunctive remedies for invasions of privacy (including compensation for mental suffering). The Warren–Brandeis right to privacy, along with the right to be let alone, was followed in 1973 by the first affirmative government undertaking to protect privacy in the computer age. The new philosophy was expressed in the Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, published by the US Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services). This report developed the principles for ‘fair information practices’ that were subsequently adopted by the United States in the 1974 Privacy Act, and ultimately by the European Union in 1995 in its Data Protection Directive. The fair information practice principles established in the United States in 1973–1974 remain largely operative around the world today in regimes and societies that respect information privacy rights of individuals. The fundamental US HEW/Privacy Act principles were:

- **a** there must be no personal data record-keeping systems whose very existence is secret;
- **b** there must be a way for an individual to find out what information about him or her is in a record and how it is used;
- **c** there must be a way for an individual to prevent information about him or her obtained for one purpose from being used or made available for other purposes without his or her consent;
- **d** there must be a way for an individual to correct or amend a record of identifiable information about him or her; and
- **e** any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use, and must take reasonable precautions to prevent misuse of the data.

**Classification of data**

The definitions of personal data and sensitive personal data vary by regulation. The FTC considers information that can reasonably be used to contact or distinguish an individual (including IP addresses) to constitute personal data (at least in the context of children’s privacy). Generally, sensitive data includes personal health data, credit reports, personal information collected online from children under 13, precise location data, and information that can be used for identity theft or fraud.

**Federal laws**

Congress has passed laws protecting personal information in the most sensitive areas of consumer life, including health and financial information, information about children and credit information. Various federal agencies are tasked with rule making, oversight and enforcement of these legislative directives.
The scope of these laws and the agencies that are tasked with enforcing them is formidable. Laws such as the Children's Online Privacy Protection Act of 1998 (COPPA), the Health Insurance Portability and Accountability Act of 1996, the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA), the FCRA, the Electronic Communications Privacy Act, the Communications Act (regarding CPNI) and the Telephone Consumer Protection Act of 1991, to name just a few, prescribe specific statutory standards to protect the most sensitive consumer data.

The Cybersecurity Act, passed in 2015, includes a Cybersecurity Information Sharing Act (CISA). CISA is designed to foster cyberthreat information sharing and to provide certain liability shields related to such sharing and other cyber-preparedness. In addition, US intelligence agency collection of bulk phone metadata pursuant to the USA Freedom Act ended in 2015, which means that targeted court orders are required for government collection of phone metadata stored by telecommunications companies.

The Defend Trade Secrets Act (DTSA) also provides federal legislative protection for information by expanding access to judicial redress for unauthorised access and use of trade secrets. The DTSA amends the Economic Espionage Act of 1996 to provide plaintiffs with a private cause of action to sue for trade-secret theft and pursue damages in federal court. The DTSA authorises a federal court to grant an injunction to prevent actual or threatened misappropriation of trade secrets, but the injunction may not prevent a person from entering into an employment relationship; nor place conditions on employment based merely on information the person knows. Rather, any conditions placed on employment must be ‘based on evidence of threatened misappropriation’. Moreover, the DTSA precludes the court from issuing an injunction that would ‘otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business’.

**State laws**

In addition to the concurrent authority that state attorneys general share for enforcement of certain federal privacy laws, state legislatures have been especially active on privacy issues that states view worthy of targeted legislation. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues, cyberstalking, data disposal, privacy policies, security breach notification, employer access to employee social media accounts, unsolicited commercial communications and electronic solicitation of children, to name but a few.

California is viewed as a leading legislator in the privacy arena, and its large population and high-tech sector means that the requirements of California law receive particular attention.

---

and often have *de facto* application to businesses operating across the United States. The combined legislative and enforcement authority of the federal and state governments ensures that the policy leadership articulated at the federal level – like the White House’s 2012 Privacy Report – can be implemented effectively in practice.

**Co-regulation and industry self-regulation**

To address concerns about privacy practices in various industries, industry stakeholders have worked with the government, academics and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively developed accountability programmes establish expected practices for use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. This approach has had notable success, such as the development of the ‘About Advertising’ icon by the Digital Advertising Alliance and the opt-out for cookies set forth by the Network Advertising Initiative. Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. The same is true for companies that publish privacy policies – a company’s failure to comply with its own privacy policy is a quintessentially deceptive practice. It should also be noted that various laws require publication or provision of privacy policies, including, *inter alia*, the GLBA (financial data), Health Insurance Portability and Accountability Act (HIPAA) (health data) and California law (websites collecting personal information). In addition, voluntary membership or certification in various self-regulatory initiatives also require posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on those policies.

**ii General obligations for data handlers**

There is no general requirement to register databases in the United States. Depending on the context, data handlers may be required to provide data subjects with a pre-collection notice, and the opportunity to opt out of the use and disclosure of regulated personal information. Information that is considered sensitive personal information, such as health information, may involve opt-in rules. The FTC considers it a deceptive trade practice if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was obtained.

**iii Technological innovation and privacy law**

Electronic marketing is extensively regulated in the United States through a myriad of laws. The CAN-SPAM Act is a federal law governing commercial email messages. Generally, a company is permitted to send commercial emails to anyone under CAN-SPAM, provided these conditions are met: the recipient has not opted out of receiving such emails from the

---

10 See oag.ca.gov/privacy/privacy-laws.
11 See www.aboutads.info; www.networkadvertising.org/choices/?partnerId=1/.
company, the email identifies the sender and the sender’s contact information, and the email has instructions on how to easily and at no cost opt out of future commercial emails from the company.

Generally, express written consent is required for companies to send marketing text messages. Marketing texts are a significant class action risk area.

There is no specific federal law that regulates the use of cookies and other similar online tracking tools. However, the use of tracking mechanisms should be carefully and fully disclosed in a company’s website privacy policy. Additionally, it is best practice for websites that allow online behavioural advertising to participate in the Digital Advertising Alliance code of conduct, which enables users to easily opt out of being tracked for these purposes. California law imposes further requirements on online tracking. California requires companies that track personally identifiable information over time and multiple websites to disclose how the company responds to ‘do-not-track’ signals, and whether users can opt out of such tracking.

Location tracking is currently a subject of interest and debate. FCC regulations govern the collection and disclosure of certain location tracking by telecommunications providers (generally speaking, telephone carriers). Additionally, the FTC and California have issued best-practice recommendations for mobile apps and mobile app platforms.

**iv Specific regulatory areas**

The US system of privacy is composed of laws and regulations that focus on particular industries (financial services, healthcare, communications), particular activities (i.e., collecting information about children online) and particular types of data.

**Federal**

*Financial privacy*

For financial privacy, the federal banking agencies and the FTC were previously primarily responsible for enforcing consumer privacy under the GLBA, which applies to financial institutions. Following the 2010 Dodd-Frank legislation, such laws will be primarily (but not exclusively) enforced by the new Consumer Financial Protection Bureau, which has significant, independent regulatory and enforcement powers. The FTC, however, will remain primarily responsible for administering the FCRA, along with the general unfair and deceptive acts and practices standards under the FTCA and COPPA, which impose affirmative privacy and security duties on entities that collect personal information from children under 13 years of age.

The GLBA addresses financial data privacy and security by establishing standards for safeguarding customers’ ‘non-public personal information’ – or personally identifiable financial information – stored by ‘financial institutions’, and by requiring financial institutions to provide notice of their information-sharing practices. In brief, the GLBA requires financial institutions to provide notices of policies and practices regarding disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties, unless consumers are provided the right to opt out of such disclosure or other exceptions apply; and to establish safeguards to protect the security of personal information.

The FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003, imposes requirements on entities that possess or maintain consumer credit reporting information, or information generated from consumer credit reports. Consumer reports are ‘any written, oral, or other communication of any information by a consumer reporting
agency bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for credit, insurance, employment or other similar purposes. The FCRA mandates accurate and relevant data collection to give consumers the ability to access and correct their credit information, and limits the use of consumer reports to permissible purposes such as employment, and extension of credit or insurance.¹²

**Healthcare privacy**

For healthcare privacy, agencies within the Department of Health and Human Services administer and enforce HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). HIPAA was enacted to create national standards for electronic healthcare transactions, and the US Department of Health and Human Services has promulgated regulations to protect privacy and security of personal health information (PHI). Patients generally have to opt in before their information can be shared with other organisations.¹³ HIPAA applies to ‘covered entities’, which include health plans, healthcare clearing houses and healthcare providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.

‘Protected health information’ is defined broadly as ‘individually identifiable health information [. . .] transmitted or maintained in electronic media’ or in ‘any other form or medium’. ‘Individually identifiable health information’ is defined as information that is a subset of health information, including demographic information that ‘is created or received by a health care provider, health plan, employer, or health care clearinghouse’; that ‘relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual’; and that either identifies the individual or provides a reasonable means by which to identify the individual. HIPAA also does not apply to ‘de-identified’ data.

A ‘business associate’ is an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities). Business associates are required to enter into agreements, called business associate agreements, requiring business associates to use and disclose PHI only as permitted or required by the business associate agreement or as required by law, and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement, as well as numerous other provisions regarding confidentiality, integrity and availability of electronic PHI. HIPAA and HITECH not only restrict access to and use of medical information, but also impose stringent information security standards.


Communications privacy

For communications privacy, the FCC, the Department of Justice and, to a considerable extent, private plaintiffs can enforce the data protection standards in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and various sections of the Communications Act, which include specific protection for CPNI such as telephone call records. The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communications and related records. The Computer Fraud and Abuse Act prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks. The FCC, however, is the primary regulator for communications privacy issues, and has been active over the past year.

The FCC shares jurisdiction with the FTC on certain privacy and data security issues, including notably on the issue of robocalls as governed by the Telephone Consumer Protection Act. There has been significant regulatory activity in the past year, including guidance released by the FCC on auto-diallers in August 2015, not to mention substantial private litigation driven by the statutory penalties provided for by the Telephone Consumer Protection Act (TCPA). The FCC has stated that complaints regarding unwanted calls are the largest category of complaints received by the FCC – numbering over 215,000 complaints in 2014 alone.14

The FCC entered a $595,000 settlement with Cox Communications for Cox’s failure to protect its customers’ personal information during a breach. A hacker allegedly accessed the personal information of 61 Cox subscribers during a 2014 breach, and shared the information on social media sites and with other hackers. This settlement was the FCC’s first security enforcement action with a cable company, and includes significant compliance programme requirements. It is another reminder that the FCC is now an aggressive player in the cybersecurity arena, even for relatively minor incidents, and that the CPNI rules include breach notification requirements.

Children’s privacy

COPPA applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires that these website operators post a privacy policy, provide notice about collection to parents, obtain verifiable parental consent before collecting personal information from children, and other actions.15

Other federal privacy laws

Even the array of privacy laws described above is hardly comprehensive. A number of other federal privacy laws protect personal information in the areas of cable television, education, telecommunications customer information, drivers’ and motor vehicle records, and video rentals. Federal laws also protect marketing activities such as telemarketing, junk

---

15 Available at www.law.cornell.edu/USCode/text/15/6501.
faxes and unsolicited commercial email. In addition, in October 2016, the Department of Transportation issued guidance on cybersecurity best practices for interconnected cars and self-driving technology.

**State legislation**

In the areas of online privacy and data security alone, state legislatures have passed a number of laws covering access to employee and student social media passwords, children's online privacy, e-Reader privacy, online privacy policies, false and misleading statements in website privacy policies, privacy of personal information held by ISPs, notice of monitoring of employee email communications and internet access, phishing, spyware, security breaches, spam and event data recorders. California is viewed as the leading legislator in the privacy arena, with many other states following its privacy laws. State attorneys general also have concurrent authority with the FTC or other federal regulators under various federal laws, such as COPPA, HIPAA and others.

The National Council of State Legislatures summarises the following state provisions regarding online privacy:

**Privacy Policies for Websites or Online Services**
California’s Online Privacy Protection Act requires an operator [. . .] to post a conspicuous privacy policy on its Website or online service [. . .] and to comply with that policy. The law, among other things, requires that the privacy policy identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its Website [and] how the operator responds to a web browser ‘Do Not Track’ signal. Connecticut [r]equires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be ‘publicly displayed’ by posting on a web page and the policy must [. . .] protect the confidentiality of Social Security numbers.

**Privacy of Personal Information Held by Internet Service Providers**
Two states, Nevada and Minnesota, require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.

**False and Misleading Statements in Website Privacy Policies**
Nebraska prohibits knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public. Pennsylvania includes false and misleading statements in privacy policies published on Websites or otherwise distributed in its deceptive or fraudulent business practices statute.

**Notice of Monitoring of Employee E-mail Communications and Internet Access**
Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access.¹⁶

---

After Congress rescinded the FCC’s privacy rules for internet providers, several states put forth their own proposals to restrict how ISPs collect and use consumer data. Alaska, California, Connecticut, Illinois, Kansas, Maryland, Massachusetts, Minnesota, Montana, New York, Pennsylvania, Rhode Island, Vermont and Washington have all at least considered bills that would establish some control over the collection, use and sharing, of consumer data by ISPs. None of these proposals have been passed to date.

**Children’s online privacy**

California prohibits websites directed to minors from advertising products based on information specific to that minor. The law also requires the website operator to permit a minor to request removal of content or information posted on the operator’s site or service by the minor, with certain exceptions.

**IV INTERNATIONAL DATA TRANSFER**

There are no significant or generally applicable data transfer restrictions in the United States; however, the United States has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by other countries. The ruling by the CJEU that the US–EU Safe Harbor Framework is ‘invalid’ has brought a considerable degree of uncertainty to the thousands of companies that rely on it as a bedrock of day-to-day global operations. This development had a significant impact on businesses that rely on Safe Harbor to legitimise transfers of personal data from the EU to the United States.

The EU–US Privacy Shield provides a new framework for transatlantic data transfers. The new agreement, which was announced in February and activated in August, replaces Safe Harbor, which was invalidated by the European Court of Justice in October 2015. The new agreement places more stringent duties on US companies to safeguard Europeans’ personal data and on the US Department of Commerce and the FTC for increased scrutiny, enforcement and partnership with European data protection authorities. As part of the framework, the United States agrees that there will be no indiscriminate mass surveillance and access to data for law enforcement and national security purposes with respect to data transferred under the new framework, and must meet certain checks to ensure data are only accessed as necessary and proportionate. In addition, European citizens who believe their data have been compromised in violation of the new agreement will be able to bring complaints to a dedicated ombudsperson. However, some elements of the new agreement share qualities with the now-defunct Safe Harbor, including that companies will subscribe to data protection principles, and that there will be a structured redress process.

In 2012, the United States was approved as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC became the system’s first privacy enforcement authority. The FTC’s Office of International Affairs works

17 Calif Bus & Prof Code Sections 22580–22582.
with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.\textsuperscript{19} In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.\textsuperscript{20}

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management\textsuperscript{21} reveals the success of enforcement in pushing corporate privacy managers to look beyond the letter of the law to develop state-of-the-art privacy practices that anticipate FTC enforcement actions, best practices and other forms of FTC policy guidance. Many corporate privacy managers explain that the constant threat and unpredictability of future enforcement by the FTC and parallel state consumer protection officials, combined with the deterrent effect of enforcement actions against peer companies, motivate their companies to proactively develop privacy policies and practices that exceed industry standards. Other companies respond by hiring a privacy officer, or by creating or expanding a privacy leadership function. The risk of enforcement has also prompted companies to engage in ongoing dialogues with the FTC and state regulators.

Corporate privacy managers have also emphasised that while compliance-oriented laws in other jurisdictions do not always keep pace with technological innovation, the FTC’s Section 5 enforcement authority allows it to remain nimble in protecting consumer privacy as technology and consumer expectations evolve over time.

The United States does not require companies to appoint a data protection officer (although specific laws such as the GLBA and HIPAA require companies to designate employees to be responsible for the organisation’s mandated information security and privacy programmes). However, it is best practice to appoint a chief privacy officer and an IT security officer. Most businesses in the United States are required to take reasonable physical, technical and organisational measures to protect the security of sensitive personal information, such as financial or health information. An incident response plan and vendor controls are not generally required under federal laws (other than under the GLBA and HIPAA), although they are best practice in the United States and may be required under some state laws. Regular employee training regarding data security is also recommended. Under the FCC’s now judicially upheld Open Internet Order, broadband ISPs are now also likely to be expected to have incident response plans and vendor controls for data security.

Some states have enacted laws that impose additional security or privacy requirements. For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls, and California requires covered entities to have an online privacy policy with specific features, such as an effective date.

\textsuperscript{20} See ‘APEC Overview’, Chapter 2.
VI DISCOVERY AND DISCLOSURE

Companies may be required under various federal and state laws to produce information to law enforcement and regulatory authorities, and to civil litigation demands. For example, companies may be ordered to produce information based on federal or state criminal authorities issuing a search warrant, a grand jury subpoena or a trial subpoena, or federal or state regulatory authorities issuing an administrative subpoena. Further, companies could be ordered to produce information upon receiving a civil subpoena in civil litigation.

Such US legal demands may create potential conflicts with data protection or privacy law outside the United States. Companies should consider these possible conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to European data, such that European data could be considered within the company’s lawful control in the United States and thereby subject to production requests irrespective of European blocking statutes.

The United States does not have a blocking statute. Domestic authorities generally support compliance with requests for disclosure from outside the jurisdiction. The principle of comity is respected, but national law and the Federal Rules of Civil Procedure typically trump foreign law.22

In a highly significant recent case, the federal court in the Southern District of New York (Manhattan) ruled that Microsoft could be required to transfer customer communications (the contents of emails) stored in Ireland to law enforcement in the United States.23 However, in July 2016, the Second Circuit overturned the District Court’s decision, holding that the government cannot force Microsoft to turn over customer emails stored outside the United States.24 The issue in the case concerns whether a search warrant served in the United States could authorise the extraterritorial transfer of customer communications notwithstanding the laws of Ireland and the availability of the mutual legal assistance treaty process. The Second Circuit held that Microsoft would not have to turn over customer emails stored in Ireland because the warrant provision of the Stored Communications Act (SCA) does not extend to data stored on foreign servers. The Court stated that ‘Congress did not intend the SCA’s warrant provisions to apply extraterritorially’. Microsoft’s resistance to the US government’s search warrant was supported by numerous other communications and tech companies. Microsoft has hailed this decision as one that ensures people’s privacy rights are protected by the laws of their own country, as well as one that prevents foreign governments from accessing consumer data stored within the United States. This decision may also help protect the interest of US companies providing global cloudcomputing services.

The Second Circuit’s decision in Microsoft that extraterritoriality should not apply has not been followed by all courts. On 3 February 2017, Magistrate Judge Thomas Rueter, in the Eastern District of Pennsylvania, required Google Inc to comply with warrants

22 Société Nationale Industrielle Aérospatiale v. US District Court, 482 US 522, 549 (1987) (requiring a detailed comity analysis balancing domestic and foreign sovereign interests, in particular US discovery interests and foreign blocking statutes). These issues are currently being litigated in a case involving the execution of a criminal search warrant issued to Microsoft for data stored in its servers located in Ireland. The case is now on appeal following the District Court decision obliging Microsoft to produce the data in question.

23 In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp, 5 F Supp 3d 466.

24 In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp, No. 14-02985 (2nd Cir 14 July 2016).
issued pursuant to the SCA that sought emails in the accounts of two individuals. Google partially complied but refused to disclose user data stored internationally. The Court held that transferring electronic data from an overseas server to a domestic data centre is not a seizure that interferes with the customer’s possessory interest in the data and invasion of customer privacy occurs only when law enforcement reviews the data, which would be done in Pennsylvania. The Court noted that the nature of Google's data storage makes it difficult to determine the exact location of a user's data at a moment, which it believed makes the Microsoft court’s location test unworkable.

In another significant case, the Justice Department attempted to use the All Writs Act to force Apple to help it unlock the iPhone used by Syed Rizwan Farook, one of the shooters in the San Bernardino terrorist attack. However, the Department of Justice dropped the case after the FBI reportedly discovered an alternative means to access the phone by contracting with and paying $1 million to a private hacking company. It is unclear how investigators bypassed Apple's security measures, or what FBI agents learned about the plot from the content they were able to review. Reportedly, the government has decided not to disclose the vulnerability to Apple. The decision averts a judicial opinion on whether the All Writs Act permits a court to order a company to provide technical assistance – which includes compelling a company to write code – for use in unlocking encrypted devices. Many in the tech community had warned that a decision in favour of the FBI would set a dangerous precedent, violating companies’ constitutional rights and weakening privacy and security for users around the world.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Every business in the United States is subject to privacy laws and regulations at the federal level, and frequently at the state level. These privacy laws and regulations are actively enforced by federal and state authorities, as well as in private litigation. The FTC, the Executive Branch and state attorneys general also issue policy guidance on a number of general and specific privacy topics.

Like many other jurisdictions, the United States does not have a central de jure privacy regulator. Instead, a number of authorities – including, principally, the FTC and state consumer protection regulators (usually the state attorney general) – exercise broad authority to protect privacy. In this sense, the United States has more than 50 de facto privacy regulators overseeing companies’ information privacy practices. Compliance with the FTC’s guidelines and mandates on privacy issues is not necessarily coterminous with the extent of an entity’s privacy obligations under federal law – a number of other agencies, bureaux and commissions are endowed with substantive privacy enforcement authority.

Oversight of privacy is by no means exclusively the province of the federal government – state attorneys general have increasingly established themselves in this space, often drawing from authorities and mandates similar to those of the FTC. The plaintiff’s bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of corporations doing business with consumers.

At the federal level, Congress has passed robust laws protecting consumers’ sensitive personal information, including health and financial information, information about children
and credit information. At the state level, nearly all 50 states have data breach notification laws on the books,25 and many state legislatures – notably California26 – have passed privacy laws that typically affect businesses operating throughout the United States.27

**FTC**

The FTC is the most influential government body that enforces privacy and data protection28 in the United States.29 It oversees essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.30 Through exercise of powers arising out of Section 5 of the FTCA, the FTC has taken a leading role in laying out general privacy principles for the modern economy. Section 5 charges the FTC with prohibiting ‘unfair or deceptive acts or practices in or affecting commerce’.31 The FTC’s jurisdiction spans across borders – Congress has expressly confirmed the FTC’s authority to provide redress for harm abroad caused by companies within the United States.32

Former FTC Commissioner Julie Brill noted, ‘the FTC has become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its disposal to prosecute an impressive series of enforcement cases’.33 Using this authority, the FTC has brought numerous privacy deception and unfairness cases and enforcement actions, including over 100 spam and spyware cases and approximately 60 data security cases.34

The FTC has sought and received various forms of relief for privacy related ‘wrongs’ or bad acts, including injunctive relief, damages and the increasingly popular practice of consent decrees. Such decrees require companies to unequivocally submit to the ongoing oversight of the FTC, and to implement controls, audit, and other privacy enhancing processes during a period that can span decades. These enforcement actions have been characterised as shaping a common law of privacy that guides companies’ privacy practices.35

‘Deception’ and ‘unfairness’ effectively cover the gamut of possible privacy-related actions in the marketplace. Unfairness is understood to encompass unexpected information

---

28 This discussion refers generally to ‘privacy’ even though, typically, the subject matter of an FTC action concerns ‘data protection’ more than privacy. This approach follows the usual vernacular in the United States.
30 See www.ftc.gov/about-ftc/what-we-do.
31 15 USC Section 45.
32 15 USC Section 45(a)(4).
35 See, for example, Solove and Harzog, 2014 (see footnote 29).
practices, such as inadequate disclosure or actions that a consumer would find ‘surprising’ in the relevant context. The FTC has taken action against companies for deception when false promises, such as those relating to security procedures that are purportedly in place, have not been honoured or implemented in practice. As part of this new common law of privacy (which has developed quite aggressively in the absence of judicial review), the FTC’s enforcement actions include both online and offline consumer privacy practices across a variety of industries, and often target emerging technologies such as the internet of things.

The agency’s orders generally provide for ongoing monitoring by the FTC, prohibit further violations of the law and subject businesses to substantial financial penalties for order violations. The orders protect all consumers dealing with a business, not just the consumers who complained about the problem. The FTC also has jurisdiction to protect consumers worldwide from practices taking place in the United States – Congress has expressly confirmed the FTC’s authority to redress harm abroad caused from within the United States.\(^{36}\)

The states

Similarly to the FTC, state attorneys general retain powers to prohibit unfair or deceptive trade practices arising from powers granted by ‘unfair or deceptive acts and practices’ statutes. Recent privacy events have seen increased cooperation and coordination in enforcement among state attorneys general, whereby multiple states will jointly pursue actions against companies that experience data breaches or other privacy allegations. Coordinated actions among state attorneys general often exact greater penalties from companies than would typically be obtained by a single enforcement authority. In the past two years, several state attorneys general have formally created units charged with the oversight of privacy, in states such as California, Connecticut and Maryland.

The mini FTCAs in 43 states and the District of Columbia include a broad prohibition against deception that is enforceable by both consumers and a state agency. In 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

ii Recent enforcement cases

FTC data protection enforcement

The FTC’s data protection enforcement has spanned both privacy and security cases, and has focused on both large and small companies across a variety of industries. Some illustrative cases are summarised below.

Internet of things

The FTC recently broke new ground by bringing an enforcement action in the emerging field of the ‘internet of things’. In September 2013, the FTC announced that it settled a case with TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely. The FTC’s complaint charged that the company falsely claimed in numerous product descriptions that its cameras were ‘secure’; in reality, the cameras were equipped with faulty software that permitted anyone with the cameras’ internet address to watch or listen online. As a result, hundreds of consumers’ private camera feeds were made public on the internet. The FTC’s order imposes numerous requirements on TRENDnet:

\(^{36}\) 15 USC Section 45(a)(4).
a prohibition against misrepresenting the security of its cameras;  
b the establishment of a comprehensive information security programme designed to address security risks;  
c submitting to third-party assessments of its security programmes every two years for the next 20 years;  
d notifying customers of security issues with the cameras and the availability of the software update to correct them; and  
e providing customers with free technical support for the next two years.  

The FTC issued a report on the internet of things, ‘Internet of Things: Privacy & Security in a Connected World’, in 2015. Two years in the making, the report provides recommendations to companies about protecting consumer privacy and securing customer data created by the new world of sensors and wearables – mainly by building security into products and services, minimising data collection, and giving consumers notice and choice about how their data are used. The report considers new statutes to be premature, but does suggest that the agency intends to adapt existing authorities under the FTCA, the FCRA and COPPA. Republican Commissioner Wright dissented from the report, arguing that the FTC should not issue recommendations and best practices without engaging in a cost–benefit analysis to determine that such measures would, if adopted, improve consumer welfare. Commissioner Wright also suggested that the Commission departed from standard practice by issuing policy recommendations in a workshop report, as such reports typically serve only to ‘synthesise the record developed during the proceedings’. Addressing attendees at the Better Business 2016 Conference in Washington, DC on 21 April 2016, Federal Trade Commissioner Maureen Ohlhausen remarked that the Commission should examine existing privacy regulations to determine how they apply to the potential new privacy risks created by the internet of things. Commissioner Ohlhausen expressed excitement about the potential benefits that smart devices can bring, but cautioned that these technologies carry with them new risks with respect to data collection and surveillance.

Last year, the FTC published another report, entitled ‘Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues’. The report focused on how big data are used after being collected and analysed, and presented questions for businesses to consider to avoid exclusionary or discriminatory outcomes for consumers. The report discussed innovative uses of big data that are benefitting underserved populations, such as through increased educational and healthcare opportunities, but also looked at risks that could arise from biases about certain groups. The report discusses numerous factors for companies to consider to enhance the relevance, quality, accuracy, objectivity and fairness of predictions and decision-making based on big-data analytics and embedded algorithms.

Financial and medical information

The SEC Office of Compliance Inspections and Examinations (OCIE) issued guidance on cybersecurity and announced examination priorities, taking multiple steps to heighten its enforcement presence for cybersecurity matters. The SEC took several cybersecurity-related steps in September 2015 that related to its mandate to oversee investment advisers and

broker-dealers, and to protect investors. OCIE issued a risk alert setting forth concrete guidance for broker-dealers and investment advisers, including notably a view that multifactor authentication was a ‘basic control’. The alert served to announce cybersecurity as a renewed area of focus for examinations, and included a sample document request for upcoming exams. Further, the SEC announced that it reached a settlement with R T Jones, an investment adviser that did not have cybersecurity policies and procedures in place prior to a breach. Despite the company’s immediate remedial steps, the SEC found that R T Jones’s failure to maintain such policies was a violation of Regulation S-P. In connection with the settlement, the Office of Investor Education and Advocacy announced an investor alert to heighten individual awareness regarding response to identity theft or data breaches impacting their investment accounts. In August 2017, OCIE issued a summary of observations from recent sweep exams of broker-dealers, investment advisers and funds. OCIE reported an improvement in awareness of cyber risks and implementation of cybersecurity practices in the past few years. Nearly all entities examined maintained written cybersecurity policies and procedures. OCIE noted, however, that many policies were not sufficiently detailed and were overly vague, and recommended that policies should be ‘reasonably tailored’ to the company. There were also noted issues with companies failing to follow their written policies, follow up with remediation when issues were discovered or patch systems appropriately.

**Mini FTCA privacy enforcement cases**

In the past few years, state attorneys general have brought a number of enforcement actions pursuant to their authority under their respective states’ mini FTCA s. Two illustrative examples are summarised below.

**Google Street View settlement**

Thirty-eight state attorneys general reached a $7 million settlement with Google over allegations that the company violated people’s privacy by collecting wi-fi data as part of its Street View activities. Google agreed to train its employees about privacy and confidentiality for at least the next 10 years, and to destroy or secure any improperly collected information.38

**Safari cookie settlements**

In 2013, 37 states settled, for $17 million, an investigation with Google involving allegations that the company bypassed web browser privacy settings to collect consumers’ browsing information. Another settlement related to this incident, which was already approved by a judge and requires Google to donate more than $3 million to schools and non-profits, is now being criticised by attorneys general from 11 states, who argue that the settlement should provide for the money to go to the people who were allegedly affected.

**Robocalls**

The FCC remains interested in preventing robocalls. The FCC issued its biannual warning to political campaigns about robocalls and text abuse in March 2016. The FCC’s warning said

the FCC ‘is committed to protecting consumers from harassing, intrusive, and unwanted robocalls and texts, including to cell phones and other mobile devices’. The warning pledged that the FCC’s Enforcement Bureau will ‘rigorously enforce’ the TCPA.

**Unsolicited faxes**

The FCC imposed a $1.84 million penalty against Scott Malcolm, DSM Supply and Somaticare for sending 115 unsolicited fax advertisements to the fax machines of 26 consumers. The faxes were primarily sent to healthcare practitioners. The FCC issued this forfeiture order in February 2016.

**iii Private litigation**

Privacy rights have long been recognised and protected by common law. The legal scholar William Prosser created a taxonomy of four privacy torts in his 1960 article ‘Privacy’ and later codified the same in the American Law Institute’s Restatement (Second) of Torts. The four actions for which an aggrieved party can bring a civil suit are:

a  intrusion upon seclusion or solitude, or into private affairs;

b  public disclosure of embarrassing private facts;

c  publicity that places a person in a false light in the public eye; and

d  appropriation of one’s name or likeness.

These rights protect not only the potential abuse of information, but generally govern its collection and use.

**The plaintiff’s bar**

The plaintiff’s bar is highly incentivised to vindicate commercial privacy rights through consumer class action litigation. The wave of lawsuits that a company faces after being accused in the media of misusing consumer data, being victimised by a hacker or suffering a data breach incident is well known across the country. A plaintiff’s litigation around the Video Privacy Protection Act (VPPA) may attempt to take advantage of a narrow opening in the First Circuit, which broadens the statute’s definition of personally identifiable information to find liability against companies that disclose information about consumers’ video viewing. In *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit held that ‘personally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual’s video-viewing behavior’. This narrow definition of personally identifiable information is upheld across numerous jurisdictions. However, this creates a circuit split with the First Circuit, which held in *Yershov v. Gannett Satellite Information Network Inc* that the VPPA was violated when a company disclosed a unique anonymous Adobe ID, GPS coordinates and video title information without consent to a third party.

**Role of courts**

Courts remain central to defining and reshaping the contours of privacy rights and remedies. This role goes beyond the role of trial courts in adjudicating claims brought by regulators

---

40  820 F3d 482, 489-90 (1st Cir 29 April 2016).
and private parties that seek to protect and define privacy rights and remedies; interest in these issues has been expressed at the highest levels. The Supreme Court has demonstrated recent interest on commercial privacy matters; in *Spokeo, Inc. v. Robins*, the Supreme Court held that an injury suffered under the FCRA must be sufficiently ‘concrete’ to find standing (discussed above). The Court held that a bare procedural violation was insufficient for proper standing. Additionally, in a November 2013 dismissal of a petition for *certiorari*, Chief Justice Roberts noted in *dicta* what issues the Court might consider when evaluating the fairness of class action remedies brought by plaintiffs challenging a privacy settlement.\textsuperscript{41} Consumer protection regulators like the FTC and state attorneys general are becoming increasingly aggressive, both in terms of the scope of enforcement jurisdiction and the stringency of regulator expectations.

**VIII  CONSIDERATIONS FOR FOREIGN ORGANISATIONS**

Foreign organisations can face a federal or state regulatory action or private action if the organisation satisfies normal jurisdictional requirements under US law. Jurisdiction typically requires minimum contacts with or presence in the United States. Additionally, a foreign organisation could be subject to sector-specific laws if the organisation satisfies that law’s trigger. For example, if a foreign organisation engages in interstate commerce in the United States, the FTC has jurisdiction. If a foreign organisation is a publicly traded company, the SEC has jurisdiction. If an organisation is a healthcare provider, the Department of Health and Human Services has jurisdiction.

Additionally, foreign organisations must consider the residency of their data subjects. Massachusetts information security regulations apply whenever an organisation processes data of Massachusetts residents. Since Massachusetts was among the first states to enact information security requirements, it has become *a de facto* national standard.

The United States does not have a general data localisation requirement, although certain requirements do exist for government contractors. Although the United States does generally require data localisation, it requires vendor oversight to ensure reasonable standards of data care. Foreign organisations operating in the United States should know that they are the responsible party under US law even if data processing is handled by a vendor outside the United States.

The United States does not have any jurisdictional issues for multinational organisations related to cloud computing, human resources and internal investigations. However, foreign organisations subject to US law should carefully consider how their data network is structured, and ensure they can efficiently respond to international data transfer needs, including for legal process. The United States respects comity, but a foreign country’s blocking statute does not trump a US legal requirement to produce information.

**IX  CYBERSECURITY AND DATA BREACHES**

Cybersecurity has been the focus of intense attention in the United States in recent years, and the legal landscape is dynamic and rapidly evolving. Public discourse has tended to conflate distinct legal issues into a single conversation that falls under the blanket term

‘cybersecurity’. Cybersecurity law and policy are more accurately described and characterised in distinct buckets: primarily consumer or personal information on the one hand, and critical infrastructure or sensitive corporate data on the other. Of course, the same or similar safeguards provide protection in both contexts.

While the United States does not have an omnibus law that governs data security, an overlapping and comprehensive set of laws enforced by federal and state agencies provides for the security of this information. These information security safeguards for personal and consumer information, as well as data breach notification provisions, are prescribed in the federal GLBA (financial data), HIPAA (healthcare data) and 47 state laws, plus the laws of numerous US territories and districts such as the District of Columbia (for broad categories of sensitive personal information). The GLBA, HIPAA and Massachusetts state law provide the most detailed and rigorous information security safeguards. The emergence of the National Institute for Standards and Technology (NIST) cybersecurity framework, as detailed below, is likely to emerge as the predominant framework under which companies undertake to ensure information security.

Forty-seven states have enacted data breach notification laws, which have varying notification thresholds and requirements. These laws generally require that individuals be notified, usually by mail (although alternate notice provisions exist), of incidents in which their personal information has been compromised. These laws usually include a notification trigger involving the compromise of the name of an individual and a second, sensitive data element such as date of birth or credit card account number.

The GLBA Safeguards Rule requires financial institutions to protect the security and confidentiality of their customers’ personal information, such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers. The Safeguards Rule requires companies to develop a written information security plan that is appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

a designate an employee to coordinate its information security programme;
b conduct a risk assessment for risks to customer information in each relevant area of the company’s operation and evaluate the effectiveness of the current safeguards for controlling these risks;
c design and implement a safeguards programme, and regularly monitor and test it;
d select service providers that can maintain appropriate safeguards, contractually require them to maintain such safeguards and oversee their handling of customer information; and
e evaluate and adjust the programme in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring.43

The SEC has broad investigative and enforcement powers over public companies that have issued securities that are subject to the Securities Acts, and enforce this authority through the use of a number of statutes, including Sarbanes-Oxley. The SEC has investigated companies

---

that are public issuers that have suffered cybersecurity incidents, including Target, and has considered theories, including that material risks were not appropriately disclosed and reported pursuant to the agency’s guidance on how and when to disclose material cybersecurity risk; and that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. The SEC also enforces Regulation S-P, which implements the privacy and security provisions of the GLBA for entities subject to its direct regulatory jurisdiction (such as broker-dealers and investment advisers). In 2015, the SEC and its ‘self-regulatory’ counterpart, the Financial Industry Regulatory Authority, issued guidance and ‘sweep’ reports regarding the state of data security among broker-dealers and investment advisers.

The Department of Health and Human Services administers the HIPAA Breach Notification Rule, which imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI maintained by entities covered by the statute (covered entities) and their business associates. The HIPAA Security Rule also requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI.

In April 2015, the Department of Justice issued its own guide, Best Practices for Victim Response and Reporting of Cyber Incidents. The Department noted concerns about working with law enforcement after suffering a data breach: ‘Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harbouring such concerns should not hesitate to contact law enforcement.’

Several states also require companies operating within that state to adhere to information security standards. The most detailed and strict of these laws is the Massachusetts Data Security Regulation, which requires that companies maintain a written information security policy (commonly known as a WISP) that covers technical, administrative and physical controls for the collection of personal information.

In February 2013, President Obama issued Executive Order 13,636, ‘Improving Critical Infrastructure Cybersecurity’. This Executive Order directs the Department of Homeland Security to address cybersecurity and minimise risk in the 16 critical infrastructure sectors identified pursuant to Presidential Policy Directive 21. The Order directed the NIST to develop a cybersecurity framework, the first draft of which was released in February 2014. The NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, and ‘provides a means of expressing cybersecurity requirements to business partners and customers and help identify gaps in an organisation’s cybersecurity practices’. While the framework is voluntary and aimed at critical infrastructure, there is an increasing expectation that use of the framework (which is laudably accessible and adaptable) could become a de facto requirement for companies holding sensitive consumer or business proprietary data. Companies operating in highly regulated industries such as the defence industrial base, energy sector, healthcare providers, banks subject to detailed examinations by the Federal Financial Institutions Examination Council and investment firms that are regulated by the SEC are subject to detailed cybersecurity standards. Congress finally passed long-awaited cybersecurity legislation in December 2015, known as the Cybersecurity Act.

45 Available at www.dhs.gov/critical-infrastructure-sectors.
As previously mentioned, the new law includes CISA, which is designed to foster cyberthreat information sharing and provided certain liability shields related to such sharing and other cyber-preparedness. Specifically, CISA provides liability protection for sharing cyberthreat information with government and private parties. CISA also authorises network monitoring and other defensive measures, notwithstanding any other provision of law. In April, President Obama created the Commission on Enhancing National Security to make recommendations for the public and private sectors to improve cybersecurity. President Obama announced 12 appointees to this Commission, who have experience in both the public and private sectors. The appointees are drawn from backgrounds in, inter alia, academia, national defence, financial services, telecommunications and payment processing.

The White House released the Presidential Policy Directive on Cyber Incident Coordination (PPD-41) in July 2016. In the wake of the hacking of the Democratic National Committee (DNC), the President announced PPD-41, which codifies lines of responsibility for cyber incidents. PPD-41 defines cyber incidents to include vulnerabilities that could potentially be exploited, but limits significant cybersecurity incidents to those ‘likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people’. Regardless of whether the cyber incident occurs in the private or public sector, for significant incidents, PPD-41 provides that the Department of Justice will take the investigatory lead, with the Department of Homeland Security leading on asset protection, and the Office of the Director of National Intelligence taking the lead on intelligence support activities. The National Security Council’s Cyber Response Group will lead national policy coordination, and a ‘Unified Coordination Group’ including ‘Federal lead agencies for threat response, asset response, and intelligence support’ will coordinate national operations with private sector entities. The relevant agency will coordinate the government’s efforts to understand potential business or operational effects for private sector critical infrastructure. Field-level federal representatives may be placed within affected private entities to coordinate efforts. PPD-41 notes guiding principles of enhanced coordination and cooperation between government sectors and private entities to better safeguard national interests and improve the US response to such incidents. PPD-41 also emphasises a guiding principle of ‘respecting affected entities’, explaining that the government will defer to private entities to notify other affected private entities and the public, and will coordinate with the affected entities if a public statement is necessary to serve the government interest. The Department of Homeland Security and the Department of Justice will maintain and update an information sheet detailing how private entities may contact the government about an incident.

On 11 May 2017, the White House followed up on the 2016 PPD-41 with a cybersecurity executive order that requires further studies and outlines priorities for the current administration’s cybersecurity efforts. The executive order calls for an assessment of critical infrastructure and seeks to build the government’s cybersecurity capacities by updating old technologies and hiring more skilled technologists. It also strongly endorsed the NIST Cybersecurity Framework, requiring all agencies to use the NIST Cybersecurity Framework to manage cyber-risks. On 16 August 2017, NIST issued an updated draft of its security and privacy guidance for federal information systems, providing specific guidance on internet-of-things (IoT) devices and on how to apply this guidance outside the government sector. NIST expects to finalise the guidance in October 2017.

As detailed above, the FTC also increasingly plays the role of de facto cybersecurity enforcement agency where consumers or personal information are involved.
Section 5 of the FTCA, the Commission has stated that providing reasonable and appropriate information security is required as a ‘fair’ trade practice. State attorneys general, empowered pursuant to state-level mini FTCAs (see Sections VII.i and ii), have taken a similar approach. Essentially, every major data breach is investigated by the FTC and state attorneys general, and may also draw the attention of other regulators such as the SEC. New York’s Department of Financial Services (DFS) issued a proposed rule in September, which would require banks, insurance companies and other financial service institutions regulated by New York’s DFS to create and maintain a cybersecurity programme designed to protect consumers and New York’s financial industry. The New York DFS rule went into full effect on 28 August 2017, requiring that all financial institutions regulated by DFS create a cybersecurity program that is approved by the board or a senior corporate official, appoint a chief information security officer, limit access to non-public data, and implement guidelines to notify state regulators of cybersecurity or data security incidents within 72 hours.

Cybersecurity remains a headline issue. In September and December 2016, Yahoo! announced that data associated with at least 500 million user accounts were stolen by what was later confirmed to be a state-sponsored actor. In December 2016, Yahoo! announced a second breach affecting 1 billion users that dated back to 2013. These two incidents are considered as possibly the largest cybersecurity breaches ever reported. The FBI announced on 11 August 2016 that it is nearly certain that the hacking of the Democratic Party in late July was the work of the Russian government. The federal investigation of the hack revealed that, in addition to the DNC and to the Democratic Congressional Campaign Committee, other party-affiliated groups were targeted in the hack, which probably included the breach of personal email accounts of the groups and group leaders. On 20 March 2017, after the 2016 election and inauguration of President Donald Trump, the FBI confirmed that it was investigating the Russian government’s interference in the 2016 election. In September 2017, the consumer reporting agency Equifax announced that the sensitive financial information of 143 million Americans had been exposed to hackers that exploited an unpatched website vulnerability. Given the pivotal role of credit bureaux such as Equifax, the ramifications of this breach may impact decision-making in the consumer financial sector.

This year has seen settlements in data breach litigation that underscore the potential financial impact of breaches. Home Depot settled an investor suit over its 2014 data breach and Neiman Marcus settled a consumer class action over its 2014 breach. Target and Nationwide agreed to settle multi-state attorneys general inquiries into their breaches for $18.5 million and $5.5 million respectively. This is on top of the $39 million Target already paid to settle with financial institutions and its $10 million settlement with a class of consumers. Numerous consumer and shareholder actions are pending against Yahoo!, including one consumer case where some allegations survived a motion to dismiss, and one shareholder action where the court declined to enjoin the sale of Yahoo!’s internet business to Verizon.

X OUTLOOK

Cybersecurity remains an intense focus of the federal government, with President Trump’s executive order continuing and expanding the work started by President Obama’s executive order addressing malicious cyberattacks. Major data breaches and attacks affecting both the private sector and public sector, including election-related hacking, have made cybersecurity risks a subject of even more universal concern for the American population. This trend is only
expected to continue and grow with an increased focus on the risks related to IoT, stemming from last year’s cybersecurity attack and the growing interest in the regulation of connected devices, starting with cars and medical devices.

The emergence of and dependence on the NIST Cybersecurity Framework as a way of evaluating and understanding companies’ cybersecurity is only expected to grow in the coming year, with new guidance explaining how to better apply the framework in the private sector and across all connected devices. This focus on the NIST Cybersecurity Framework, along with growing discussion of what companies must do to achieve reasonable security should lead to more attention to companies’ cybersecurity measures, both internally, from boards and executives, and externally, from regulators, such as the FTC.

With regard to privacy regulation of internet, telecom and tech companies, there is no certain direction where new regulators appointed by the Trump administration will head. Privacy has not been an especially partisan issue in the United States to date. Acting FTC Chairman Maureen Ohlhausen has, however, clearly articulated a philosophy of regulating privacy risks that cause real harm to individuals, rather than those that present only intangible or abstract concerns devoid of actual injury.

As of the end of 2017, the legal standards for protecting citizens against hacking are still unformed. The FTC and other relevant regulators and enforcement agencies expect companies to provide reasonable security, but what that means when no company or government department is immune from successful attack remains confusing.

Finally, the year ahead is likely to bring increased attention to connected devices, autonomous vehicles, machine learning, big-data analytics and predictive algorithms. These novel areas hold serious implications for security (as in hacking cars or medical devices), as well as with regard to personal privacy and profiling. The field of privacy, data protection and cybersecurity will continue to eschew equilibrium.
ABOUT THE AUTHORS

DIEGO ACOSTA-CHIN
_Santamaria y Steta, SC_

Mr Acosta-Chin obtained his law degree from the Monterrey Institute of Technology and Higher Education in 2008. He is fluent in Spanish and English.

Mr Acosta-Chin joined Santamarina y Steta, SC in 2009 and since then his professional practice has been focused on corporate matters, including mergers and acquisitions, data privacy matters, the prevention of money laundering, e-commerce and foreign investment.

Mr Acosta-Chin’s practice focuses on data privacy matters and he advises clients on analyses of the implications of, and actions necessary for compliance with, data privacy legislation, including the drafting and filing of writs with respect to official communications issued by the National Institute of Transparency, Access to Information and Protection of Personal Data regarding its surveillance and enforcement divisions, mapping of the processing of personal data throughout different departments or business units of an organisation, drafting the required documents to comply with the law, coordinating efforts to be in compliance with the law, advising on breaches of personal data confidentiality obligations and implementing cross-border contingency plans to mitigate and prevent security breaches, among other matters.

SETH AZUBUIKE
_Perchstone & Graeys_

Seth Azubuike is an associate at Perchstone & Graeys. His core practice areas in the firm include banking and finance, ICT and telecommunications.

Seth has been involved in high-profile transactions spanning banking and finance, ICT and telecommunications. He currently advises both the public and private sectors on the various legal issues and risk arising from banking and finance, and ICT-related transactions.

Seth has also played a key role in legislative drafting and, in particular, in driving the inclusion of certain key enactments that are crucial to the growth and development of the financial and ICT sectors in Nigeria. His interest in the development of Nigerian law is reflected in his contributions to various banking and finance and ICT publications.
INÊS ANTAS DE BARROS
VdA Vieira de Almeida
Inês Antas de Barros is a managing associate and an integral member of the telecoms, media and IT, privacy, data protection and cybersecurity practice group. Inês has been admitted as a legal expert to the European Privacy Seal. She has been involved in privacy compliance programmes and other privacy projects that raise complex issues across multiple jurisdictions and legal and regulatory areas (including health, pharmaceuticals, insurance, banking and telecommunications).

REYES BERMEJO BOSCH
Uría Menéndez Abogados, SLP
Reyes Bermejo is a lawyer in the Madrid office of Uría Menéndez. She became a lawyer in 2006 and joined the firm in 2011.

She focuses her practice on data protection, e-commerce and IT. Reyes provides national and multinational companies with day-to-day advice in the above-mentioned areas, on matters such as privacy, consumer protection and e-commerce, and dealings with public authorities, including the drafting and negotiation of IT agreements. In particular, she has extensive experience in the data protection design of commercial and M&A transactions, in the preparation of notices, clauses, contracts, protocols and training programmes, in authorisation proceedings for international transfers and administrative and judicial proceedings, and in preparing website terms and conditions and cookie policies and in advising on direct marketing activities by electronic means.

Reyes is also a professor of data protection and e-commerce law on various master’s degree programmes and seminars (the University of Valencia, and the Financial and Stock Market Studies Foundation and CEU Cardenal Herrera University, both also in Valencia).

She contributes to the firm’s data protection newsletter and legal magazine (Actualidad Jurídica Uría Menéndez) on aspects of and updates relating to data protection regulatory issues and case law.

FRANCESCA BLYTHE
Sidley Austin LLP
Francesca Blythe is an associate in the London office at Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

SHAUN BROWN
nNovation LLP
Shaun Brown is a partner with nNovation LLP, an Ottawa-based law firm that specialises in regulatory matters. With several years of experience in both the public and private sectors, Shaun's practice focuses on e-commerce, e-marketing, privacy, access to information and information security. Shaun assists clients by developing practical and effective risk-mitigation strategies, and by representing clients before tribunals and in litigation-related matters. Shaun has a deep understanding of the online marketing industry from both a technical
and legal perspective. He speaks and writes regularly on privacy, marketing and information management issues, and is the co-editor and co-author of PrivacyScan, one of Canada’s most popular and insightful resources on Canadian privacy issues.

CHRISTOPHE CLARENC
Duclos, Thorne, Mollet-Viéville & Associés (DTMV)

Christophe Clarenc is an independent lawyer working with DTMV and he specialises in digital law, information system and data security, and electronic communications.

MAGDA COCCO
VdA Vieira de Almeida

Magda Cocco is one of the partners in charge of the telecoms, media and IT practice, and is also head of the privacy, data protection and cybersecurity practice group. She has vast experience in the telecommunications sector in a variety of jurisdictions, with a special focus on Portuguese-speaking countries. In the data protection and cybersecurity sector, Magda has been involved in several public projects, providing expert advice both to private companies and public entities, and coordinating several compliance programmes in these areas.

ELLYCE R COOPER
Sidley Austin LLP

Ellyce Cooper is a partner in the firm’s Century City office and a member of the complex commercial litigation and privacy and cybersecurity practices. Ellyce has extensive experience in handling government enforcement matters and internal investigations as well as complex civil litigation. She assists companies facing significant investigations and assesses issues to determine a strategy going forward. Ellyce’s diverse experience includes representing clients in internal investigations and government investigations along with responding to and coordinating crisis situations. Her client list includes notable companies from the healthcare, pharmaceutical, accounting, financial, defence and automotive industries. Ellyce earned her JD from the University of California, Los Angeles School of Law and her BA, magna cum laude, from the University of California Berkeley.

CÉSAR G CRUZ-AYALA
Santamarina y Steta, SC

Mr Cruz-Ayala obtained his law degree from the University of Monterrey faculty of law in May 1994, which was followed by a master’s in comparative jurisprudence at New York University School of Law in May 1998. He is fluent in Spanish and English.

Mr Cruz-Ayala joined Santamarina y Steta, SC in 1993 and became a partner in 2006. During that time, his professional practice has been focused on mergers and acquisitions, data privacy matters, prevention of money laundering, and e-commerce, insurance, real estate and transnational business projects.

Mr Cruz-Ayala’s practice focuses on data privacy matters and he has a broad knowledge of data privacy legislation and its implications. He advises clients on assessing and complying with Mexican data privacy laws, including mapping of the processing of personal data throughout different departments or business units of an organisation, drafting the
documents required to comply with the law, coordinating efforts to be in compliance with
the law, advising on breaches of personal data confidentiality obligations and implementing
cross-border contingency plans to mitigate and prevent security breaches, among other
matters. Mr Cruz-Ayala is very active in the industry and regularly organises and participates
in seminars, webinars and conferences in this area.

SANUJ DAS
Subramaniam & Associates
Sanuj Das specialises in litigation, both IP and non-IP, and is a member of the Subramaniam &
Associates litigation team. He also handles patent revocation proceedings before the appellate
board, along with patent, trademark and design opposition proceedings. He has worked with
a diverse array of clients, including professionals and scientists from the telecommunications,
pharmaceutical, FMCG and apparels sectors. In addition to a bachelor’s degree in law, Sanuj
holds a bachelor’s and a master’s degree in pharmacy, with a specialisation in pharmaceuticals.

STEVEN DE SCHRIJVER
Astrea
Steven De Schrijver is a partner in the Brussels office of Astrea. He has more than 20 years of
experience advising some of the largest Belgian and foreign technology companies, as well as
innovative entrepreneurs on complex commercial agreements and projects dealing with new
technologies. His expertise includes e-commerce, software licensing, website development
and hosting, privacy law, IT security, technology transfers, digital signatures, IT outsourcing,
cloud computing, advertising, drones, robotics and social networking.

Steven has also been involved in several national and cross-border transactions in the IT,
media and telecom sectors. He participated in the establishment of the first mobile telephone
network in Belgium, the establishment of one of the first e-commerce platforms in Belgium,
the acquisition of the Flemish broadband cable operator and network, and the acquisition
and sale of several Belgian software and technology companies. He has also been involved in
numerous outsourcing projects and data protection (now GDPR) compliance projects.

Steven is the Belgian member of EuroITCounsel, a quality circle of independent
IT lawyers. He is also a board member of ITechLaw and the International Federation of
Computer Law Associations. In 2012, 2014 and 2017, he was awarded the Global Information
Technology Lawyer of the Year award by Who’s Who Legal and, in 2012, he received the ILO
Client Choice Award in the corporate law category for Belgium.

Steven has been admitted to the Brussels Bar. He holds a law degree from the University
of Antwerp (1992) and an LLM degree from the University of Virginia School of Law (1993).

MARISSA (XIAO) DONG
Jun He LLP
Ms Dong is a partner in the Beijing office, specialising in the areas of foreign direct investment,
mergers and acquisitions, and data protection, information and cybersecurity law. She
represents Fortune 500 corporations and other global enterprises, and Chinese state-owned
and private companies, as well as financial services firms, including private equity firms.

In her corporate law practice, Ms Dong guides inbound investors through all stages
of operating in China, from market investigation to market entry and business expansion
About the Authors

(including incorporating PRC entities and mergers and acquisitions). In addition, she represents prominent Chinese companies in outbound direct investments. Her clients include industry leaders in education, manufacturing and internet and telecommunications services.

She also advises clients on all aspects of data protection, information and cybersecurity law, with a special emphasis on information privacy (consumers, employees and patients), data security and breaches, and international data transfers. Ms Dong helps clients navigate China’s complex and sector-specific policy and regulatory landscape. Her clients include national and international information technology vendors, internet service providers, data brokers, retailers and distributors, and manufacturers of medical, industrial and consumer products.

FRANCES E FAIRCLOTH
Sidley Austin LLP

Fran Faircloth is an associate in Sidley Austin’s privacy and cybersecurity practice, where she assists clients with privacy and cybersecurity issues, including government and internal investigations. Ms Faircloth earned her law degree at Yale Law School, where she served as the managing editor of the Yale Law Journal. Before joining Sidley, she clerked for the Honourable Scott M Matheson, Jr, on the US Court of Appeals for the Tenth Circuit, and served as a fellow at the National Women’s Law Center.

ADRIÁN LUCIO FURMAN
M&M Bomchil

Adrián Furman is a partner in the mergers and acquisitions and entertainment law departments and in charge of M&M Bomchil’s intellectual property area. He joined the firm in 2000.

He graduated as a lawyer from the University of Buenos Aires in 1998. He obtained a postgraduate degree in corporate business law at the same institution, where he is also a professor of civil and commercial contracts.

He has worked on numerous cross-border transactions and regularly advises corporate clients on various issues of a contractual nature. He also has wide experience of issues of commercial fair trade and consumer protection.

During 2005 he was international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on his areas of expertise and at the Section of International Law of the American Bar Association seasonal meetings.

He has been and is a director and auditor of important companies such as PepsiCo, AMC Networks, Telefe and Mindray, among others.

He is co-chair of the International Commercial Transactions, Distribution and Franchise Committee of the Section of International Law of the American Bar Association.

His professional performance has been recognised by various specialised publications, including Chambers Latin America and Best Lawyers, and by the Latin American Corporate Counsel Association and Client Choice Awards.
BRUNO GRANZOTTO GIUSTO
*Siiqueira Castro – Advogados*

Bruno Granzotto Giusto graduated from Candido Mendes Law School in 2000. He gained a postgraduate degree in public law from Candido Mendes Law School and specialised in criminal law at Getulio Vargas Foundation (FGV/RJ). He also gained a postgraduate degree in administrative Sanionador law from the University of Valladolid (Spain) and a master’s in economic law from Candido Mendes Law School. He is a member of the Brazilian Bar Association, Rio de Janeiro section, and of the Criminology Committee of the Brazilian Bar Association, Rio de Janeiro section. He is a founding member of the Institute of Individual Protection Guarantees.

TAMÁS GÖDÖLLE
*Bogch & Partners Law Firm*

Tamás Gödölle graduated from the law faculty of Eötvös Loránd University in Budapest. He studied commercial and international private law for one year at the Ludwig Maximilian University of Munich in Germany and continued with postgraduate legal studies at Queen Mary and Westfield College, University of London (1990–1991). As a corporate, commercial and intellectual property lawyer, he has been practising in Hungary advising and representing national and multinational clients for over 24 years. Dr Gödölle has been a partner at Bogsch & Partners since 1996, where he specialises in trademark, copyright, antitrust, unfair competition and advertising matters, as well as franchise, distributor and licence contracts. He also has extensive experience in information technology, privacy, data protection and life science and media law issues. He is a member of the Budapest Bar, the Hungarian Association for the Protection of Industrial Property and Copyright (MIE), both the Hungarian and the International League of Competition Law (LIDC), ECTA, INTA, AIPPI, ITechLaw and GRUR. As well as speaking Hungarian, he is fluent in English and German.

TOMOKI ISHIARA
*Sidley Austin Nishikawa Foreign Law Joint Enterprise*

Mr Ishiara’s practice areas include intellectual property law, antitrust law, telecommunications, data security and privacy law, entertainment law, compliance/investigation, litigation and arbitration. Mr Ishiara has extensive experience in the field of intellectual property law and antitrust law, including giving advice to clients on patent, utility model, design patent, copyright and trademark matters (including advice on employee invention rules), engaging in licensing negotiations and litigation (including actions to annul trial decisions at the IP High Court and trials for patent invalidation at the Japanese Patent Office), and dealing with rapidly increasing IT-related disputes arising out of system development or maintenance M&A transactions.

JU BONG JANG
*Lee & Ko*

Ju Bong Jang is a partner in Lee & Ko’s data protection and privacy, and media and telecommunications practice groups. He is a leading expert in the areas of telecommunications and broadcasting regulations, IT, personal data protection, M&A and dispute resolution.
in related markets. Mr Jang has extensive experience in representing domestic and global IT companies in major cases involving hacking incidents and personal data leaks. He has consistently advised various domestic and multinational companies on their data privacy compliance programmes and other data privacy issues. He has also represented global IT companies in obtaining licences from the Korea Communications Commission for the provision of location-based services in Korea.

SHANTHI KANDIAH
SK Chambers

Shanthi Kandiah founded SK Chambers with the goal of creating a stand-alone regulatory firm that services individuals and entities involved at all levels of the regulatory scheme. Today, SK Chambers does just that – it is focused on delivering legal services in competition law, the full spectrum of multimedia laws, privacy and data protection matters, and anti-bribery and corruption laws, as well as capital market laws and exchange rules.

Shanthi Kandiah regularly advises many corporations in sectors such as media and telecommunications, FMCG, construction and credit reporting on privacy and data protection matters, including the following: compliance strategies that prevent and limit risk; managing risks through contracts with customers and suppliers; data protection and cyber-risk due diligence in relation to acquisitions, dispositions and third-party agreements; crisis management when a data breach occurs; investigations management – when faced with regulatory action for data security breaches; and data transfers abroad – advising on risks and issues.

She holds an LLM and a postgraduate diploma in economics for competition law, both from King’s College London.

BENJAMIN KIRSCHBAUM
Winheller Rechtsanwaltsgesellschaft mbH

Benjamin Kirschbaum is a research assistant at Winheller Attorneys at Law & Tax Advisors. At the law firm’s Berlin office, he focuses on banking law, blockchain, cryptocurrencies and cybersecurity.

ANNA KOBYŁAŃSKA
Kobylańska & Lewoszewski Kancelaria Prawna Sp J

Anna Kobylańska, an advocate with 15 years of experience, was in charge of data protection, new technologies and intellectual property in a global advisory company before joining Kobylańska & Lewoszewski as a founding partner. Anna specialises in providing advice on the protection of personal data to clients from the pharmaceuticals, financial services, media and automotive sectors. She regularly oversees projects focused on the analysis and implementation of the provisions of the GDPR. Anna co-authored the book Protecting Personal Data in the Practice of Entrepreneurs. She is also a lecturer at the H Grocujz Centre for Intellectual Property Law, in the field of personal data protection. She is a member of the INTA Committee for the Protection of Personal Data (an international association of trademark law specialists). For the past six years, Anna has been recognised by Chambers
Europe as one of leading lawyers in Poland in the TMT/data protection category. In 2017, her practice was recognised by Polish legal ranking company Polityka Insight as one of Poland’s foremost teams in the field of personal data.

JENS-MARWIN KOCH
Jens-Marwin Koch works as independent attorney in Berlin. He advises clients on IP, trademark and media law matters.

Jens-Marwin Koch used to work as head of the Berlin office of a Swiss law firm and worked for an IP boutique law firm in New York City. He is also admitted to practise as an attorney-at-law in New York.

ELENA KUKUSHKINA
Baker & McKenzie – CIS, Limited

Elena Kukushkina is a counsel and coordinator in the Moscow office labour and migration practice and is a member of the IT practice. Prior to joining Baker & McKenzie, she worked at another leading global law firm. She is recommended by Chambers Europe and The Legal 500 – EMEA for her employment work. Sources describe Ms Kukushkina as ‘fast, practical and business oriented’ as well as ‘result driven’.

Ms Kukushkina is seasoned in employment and immigration law matters and has extensive experience in representing major Russian and international companies in various labour disputes.

She provides major international and Russian companies with general employment advice, including on various recruitment and contract termination issues, workforce restructuring, executive compensation and employment benefits and general immigration and corporate advice. She also advises on a number of personal data-related issues, including general personal data protection, international data transfer, employee data protection and processing, data localisation requirements and the processing of data within internal investigations. She is also involved in employment litigation and represents clients in various labour law-related court cases and in the pretrial resolution of disputes with employees.

Ms Kukushkina is the author of a number of articles on labour and immigration law and data protection issues. She has also participated as a speaker at a number of conferences and seminars in this area.

FOLABI KUTI
Perchstone & Graeys

Folabi Kuti is a leading expert in the field of employment and labour relations with demonstrated competence in corporate commercial litigation, alternative dispute resolution, intellectual property law, insolvency and secured credit transactions.

He brings to his work penetrating insights accrued over several years of experience in core litigation and he currently oversees the litigation department of the firm. Folabi has a keen interest in the development of Nigerian law as well as those in other jurisdictions. His resourcefulness has contributed immensely to deepening the corporate and commercial advocacy practice of the firm. A prolific writer, Folabi has published articles and commentaries on a wide range of subjects, such as commercial litigation, civil procedure and literary criticism.
Folabi is a member of the Nigerian Bar Association, and the International Bar Association. He is a notary public and is registered with the Securities and Exchange Commission to practise in the Nigerian capital market.

**MARCIAN LEWSZEWIKI**

*Kobylańska & Lewoszewski Kancelaria Prawna Sp J*

Marcin Lewoszewski is a legal counsel with 10 years of experience in the field of personal data protection, e-commerce and telecommunications law. He is one of the founding partners of Kobylańska & Lewoszewski. Marcin is the author of a number of publications on personal data protection published by *Harvard Business Review* and the daily newspapers *Rzeczpospolita* and *Dziennik Gazeta Prawna*. He is the first Pole in history to have been selected by the International Association of Privacy Professionals (IAPP), an organisation of more than 10,000 experts in the field of privacy protection, as a representative of IAPP KnowledgeNet in Poland. In the course of his experience of working with the Inspector General for Personal Data Protection (GIODO), he participated in over 200 proceedings carried out by the authority. He has been recognised by *Chambers Europe* for the past five years in the TMT/data protection category as ‘an associate to watch’. Clients evaluating his work for this rating emphasise, among other things, that ‘He is very diligent and draws attention to details,’ ‘He perfectly understands business and is always ready to find legal solutions,’ and ‘He understands our needs.’ In 2015, he was honoured by *Dziennik Gazeta Prawna* as one of the best 30 lawyers in Poland under the age of 35, granting him the title of Rising Star.

**WILLIAM RM LONG**

*Sidley Austin LLP*

William RM Long is a partner in the London office of Sidley Austin LLP and heads the EU data protection and privacy practice. He advises international clients on a wide variety of data protection, privacy, cybersecurity, e-commerce and other regulatory matters.

**LETICIA LÓPEZ-LAPUENTE**

*Uría Menéndez Abogados, SLP*

Leticia López-Lapuente is a lawyer in the Madrid office of Spanish law firm Uría Menéndez. She heads the firm’s data protection and IT practice, and leads the LATAM data protection group. Leticia focuses her practice on data protection, commercial and corporate law, especially in the internet, software, e-commerce and technology sectors. She also advises on privacy law issues. Leticia provides clients operating in these sectors with day-to-day advice on regulatory, corporate and commercial matters, including the drafting and negotiation of contracts, M&A, privacy advice, consumer protection and e-commerce issues, corporate housekeeping, public procurement and RFP procedures, and dealings with public authorities. She has been involved in major transactions and assisted businesses and investors in these sectors.

She regularly speaks in national and international fora regarding personal data protection and technology, in addition to having written numerous articles on data protection-related matters.
CATALINA MALARA  

_M&M Bomchil_

Catalina Malara is a member of the mergers and acquisitions and entertainment law departments at M&M Bomchil. She graduated with honours from the University of Buenos Aires in 2016.

VIVEK K MOHAN  

_Sidley Austin LLP_

Vivek K Mohan is senior privacy and cybersecurity counsel at Apple Inc, where he is responsible for privacy and security issues associated with Apple’s products, services and corporate infrastructure. He joined Apple from the privacy, data security and information law group at Sidley Austin LLP, where he counselled clients in the technology, telecommunications, healthcare and financial services sectors. Mr Mohan is the co-editor and author of the PLI treatise ‘Cybersecurity: A Practical Guide to the Law of Cyber Risk’, published in September 2015. He has worked as an attorney at Microsoft, at the Internet Bureau of the New York State Attorney General (under a special appointment) and at General Electric’s corporate headquarters (on secondment). For five years, Mr Mohan was a resident fellow and later a non-resident associate with the Cybersecurity Project at the Harvard Kennedy School. He holds a JD from Columbia Law School and a BA from the University of California, Berkeley.

MICHAEL MORRIS  

_Allens_

Michael Morris is an expert telecommunications, technology, intellectual property and data protection lawyer, and is well known for staying on the cutting edge of legal developments in these areas for corporate and government clients in Australia. He is particularly experienced in large projects and transactions involving the procurement and delivery of ICT, business process outsourcing and ICT systems separations and business transformations. He is part of Allens’ leading practice advising on management of the full data life cycle, particularly the use, exchange, monetisation and protection of data, and he regularly advises clients across all industry sectors and the government on data security, privacy and associated issues.

GEORGY MZHAVANADZE  

_Baker & McKenzie – CIS, Limited_

Georgy Mzhavanadze is an associate in the Moscow office of Baker & McKenzie. He joined the labour and migration practice group in 2011 and is also a member of the IT practice. Mr Mzhavanadze is involved in litigation and pretrial resolution of disputes with employees and he provides advice on employee recruitment and termination, corporate restructuring, staff redundancy, disciplinary enforcement and compliance investigations, migration, cooperation with trade unions and other employment-related issues. He also provides advice
Mr Mzhavanadze is the author of a number of articles on labour and data protection law. He has also participated as a speaker at a number of conferences and seminars in this area.

UGOCHUKWU OBI
Perchstone & Graeys
Ugo Obi is a senior associate at Perchstone & Graeys. He heads the firm’s solicitors department and the information communications and technology group. He also leads the firm’s banking and finance department.

Ugo has been involved in a considerable range of transactions spanning banking and finance, power and energy, and information communications technology (ICT) and telecommunications. Ugo possesses a deep understanding of the Nigerian banking sector, the impact of local and international regulations and the convergence of ICT with the law, and he advises clients on international banking and ICT best practices.

Ugo has exceptional interest and expertise in global ICT and telecommunications law and this has served him well in his work as a foreign lawyer (on a secondment basis) at one of the top ICT law firms in India, where he was exposed to global information technology and telecoms law and practice.

KWANG BAE PARK
Lee & Ko
Kwang Bae Park is the head of Lee & Ko’s data protection and privacy (DPP) practice group, and key partner in the technologies, media and telecommunications (TMT) practice group. He is recognised as one of the foremost lawyers in the DPP and TMT practice sectors in Korea. He has consistently represented and advised various domestic and multinational companies on Korea’s data protection framework, cross-border data transfers of employee and customer data, and safeguards and data breach cases, both proactively and following incidents. He has participated in various international and domestic data privacy forums, such as the IAPP, Law Asia and the Asia Forum on Cyber Security and Privacy, and he works actively with the relevant governmental bodies with competence for new business activity, and in relation to developing issues such as big data and the internet of things.

VADIM PEREVALOV
Baker & McKenzie – CIS, Limited
Vadim Perevalov is an IT and IP associate at Baker & McKenzie’s Moscow office. He focuses on privacy, internet law, technology-related IP and a wide range of emerging IT regulatory issues. He also assists clients with various contentious matters.

Vadim Perevalov graduated from the Saint Petersburg State University with a Master of Laws in 2011. Mr Perevalov obtained his Bachelor of Laws from the same university in 2009.

Mr Perevalov has been invited as an expert to work with the Advisory Council of the Russian Data Protection Authority and is well recognised in the Russian privacy and data protection arena because of his active involvement in various industry committees and working groups. He was also appointed as an expert with the Institute of Internet
Development, which is heavily involved in internet and IT policymaking in Russia, and as an expert with the Regulatory Working Group on the Digital Privacy initiative of the Russian data protection authority, Roskomnadzor, involved in the development of new legislation on big data.

**DANIEL PITANGA BASTOS DE SOUZA**

*Siiqueira Castro – Advogados*

Daniel Pitanga Bastos de Souza graduated from the Catholic University of Salvador in 2006. He gained a postgraduate degree in intellectual property law from the Catholic University of Rio de Janeiro and specialised in entertainment law at the State University of Rio de Janeiro. He also holds an LLM in information technology and telecommunications law from the University of Southampton. He is a member of the Brazilian Bar Association, Rio de Janeiro section, and secretary general of the Industrial Property and Piracy Committee of the Brazilian Bar Association, Rio de Janeiro section. Daniel is vice chair of the ITechLaw (International Technology Law Association) Interactive Entertainment and Media Committee, and is also a lecturer in advertising and marketing law.

**ALAN CHARLES RAUL**

*Sidley Austin LLP*

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP’s highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul’s practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Data Security, Privacy & Intellectual Property Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves *ex officio* as a member of the American Bar Association’s Cybersecurity Legal Task Force, following his prior appointment to the Task Force by the ABA President. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

**HUGH REEVES**

*Walder Wyss Ltd*

Hugh Reeves is an associate in the information technology, intellectual property and competition team of the Swiss law firm Walder Wyss Ltd. His preferred areas of practice include technology transfers, copyright, patent, trademark and trade secret law, as well as information technology law. He is also active in the areas of data protection and privacy law.

Hugh Reeves was educated at the University of Lausanne (BLaw, 2008; MLaw, 2010) and the University of California at Berkeley (LLM, 2016).
GÉRALDINE SCALI  
_Sidley Austin LLP_  
Géraldine Scali is a counsel in the London office of Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

JÜRG SCHNEIDER  
_Walder Wyss Ltd_  
Jürg Schneider is a partner with the Swiss law firm Walder Wyss Ltd. Jürg Schneider’s practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. Jürg Schneider is a member of the board of directors of the International Technology Law Association and immediate past co-chair of its data protection committee. In addition, Jürg Schneider regularly publishes and lectures on ICT topics in Switzerland and abroad.

Jürg Schneider was educated at the University of Neuchâtel (lic iur 1992, Dr iur 1999). He has previously worked as a research assistant at the University of Neuchâtel, as a trainee at the legal department of the canton of Neuchâtel and in a Neuchâtel law firm.

Jürg Schneider speaks German, French and English. He is registered with the Zurich Bar Registry and admitted to practise in all of Switzerland.

MONIQUE STURNY  
_Walder Wyss Ltd_  
Monique Sturny is a senior associate in the information technology, intellectual property and competition team of the Swiss law firm Walder Wyss Ltd. She advises international and domestic companies on data protection law, competition law, distribution law, contract law and information technology law matters, as well as with respect to the setting up of compliance programmes. She represents clients in both antitrust and data protection proceedings in court and before administrative bodies. She regularly publishes and speaks at conferences in her areas of practice.

Monique Sturny was educated at the University of Fribourg (lic iur 2002), the London School of Economics and Political Science (LLM in international business law, 2007) and the University of Berne (Dr iur, 2013).

ADITI SUBRAMANIAM  
_Subramaniam & Associates_  
Aditi Subramaniam holds a bachelor’s degree in law from Merton College, University of Oxford, and is also a qualified advocate registered with the New Delhi Bar. She brings rich experience to the firm from training with highly reputed law firms in India, the United Kingdom and Australia. She has attended a number of live proceedings and trials before various tribunals and courts in India and abroad, and has also assisted advocates and senior counsel in trial preparations. She is an experienced legal researcher, author of several publications on intellectual property law and is currently training to be a litigator.
About the Authors

YUET MING THAM
Sidley Austin LLP

Yuet Ming Tham is a partner in Sidley Austin’s Hong Kong and Singapore offices. She advises international corporations on their legal risks, such as those relating to privacy, data protection and cybersecurity law issues, as well as cross-border compliance and investigations, anti-bribery laws (including FCPA), international trade controls, sanctions, anti-money laundering and dispute resolution.

Prior to joining Sidley, Yuet was the Asia head of the regulatory, compliance and investigations group, and head of the Asia life sciences group at another international law firm. She has also held roles as a deputy public prosecutor in Singapore and was the Asia Pacific regional compliance director for Pfizer. During that time, she was responsible for compliance and investigations in Singapore, Japan, China, Australia, Korea, India, Indonesia, Thailand, Taiwan, Hong Kong, Malaysia and the Philippines.

Yuet is named as a leading lawyer in *Chambers Asia-Pacific* in four categories, as well as being recognised in *IFLR1000* and *The Legal 500 – Asia Pacific*. In 2014, she was the only lawyer awarded the Client Choice award by International Law Office for white-collar crime practice in Hong Kong. The leading legal directory *Chambers Asia-Pacific* noted that industry players appreciate Yuet’s ‘wealth of knowledge of the latest trends across the region’, as well as her having a ‘tough, no-nonsense approach in tackling tricky compliance questions’. In the global edition of the book, she is described by clients as ‘a marvellous and gifted attorney’, and a client observed that ‘two things stand out about her: she is extraordinarily responsive, but is also very good at getting answers to your questions from a practical perspective. In that respect, she really is a gem of a lawyer’. Yuet has up-to-the-minute knowledge on the rapidly changing issues surrounding privacy, data protection and cybersecurity matters related to Hong Kong, Singapore and the rest of Asia. She has written several articles and is a frequent speaker at industry conferences on these subjects.

She speaks English, Mandarin, Cantonese and Malay, and is admitted to practise in Hong Kong, Singapore, New York, and England and Wales.

ARNAUD VANBREMEERSCH
Duclos, Thorne, Mollet-Viéville & Associés (DTMV)

Arnaud Vanbremeersch is a partner at DTMV and specialises in the fields of new technologies, licensing, data protection, subcontracting, joint ventures and distribution and commercial IP agreements.

NIKOLA WERRY
Winheller Rechtsanwaltsgesellschaft mbH

Nikola Werry, LLM (UK), heads the IP/IT department at Winheller Attorneys at Law & Tax Advisors, where she advises German and international companies and non-profit organisations on issues of data protection, IT law and intellectual property. She also provides legal counsel in German and international copyright, trademark and media law matters.

Nikola Werry has several years of experience gained at international business law firms (e.g., in Washington, DC, United States). Before joining Winheller, she worked in the legal department of an international Big Four accounting firm.
FRANCISCO ZAPPA

*M&M Bomchil*

Francisco Zappa is a semi-senior lawyer in the mergers and acquisitions and entertainment law departments. He joined M&M Bomchil in 2011.

He graduated with honours from the University of Salvador, Buenos Aires and completed his masters' degree in corporate law at the University of San Andrés, Buenos Aires. His practice focuses on diverse corporate and contractual matters. He has wide experience in fair trade and consumer protection issues and specialises in data protection law.

During 2017, he was an international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on matters in his areas of expertise.
CONTRIBUTING LAW FIRMS’ CONTACT DETAILS

ALLENS
Level 26
480 Queen Street
Brisbane Queensland 4000
Australia
Tel: +61 7 3334 3000
Fax: +61 7 3334 3444
michael.morris@allens.com.au
www.allens.com.au

BOGSCH & PARTNERS LAW FIRM
Királyhágó tér 8–9
1126 Budapest
Hungary
Tel: +36 1 318 1945
Fax: +36 1 318 7828
tamas.godolle@bogsch.hu
www.bogsch.hu

ASTREA
Louizalaan 235
1050 Brussels
Belgium
Tel: +32 2 215 97 58
Fax: +32 2 216 50 91
sds@astrealaw.be
www.astrealaw.be

DUCLOS, THORNE, MOLLET-VIÉVILLE & ASSOCIÉS (DTMV)
Attorneys at the Paris Bar
164 rue du Faubourg Saint-Honoré
75008 Paris
France
Tel: +33 1 56 69 31 00
Fax: +33 1 56 69 31 01
www.dtmv.com/en

BAKER & MCKENZIE – CIS, LIMITED
White Gardens, 10th floor
9 Lesnaya Street
Moscow, 125047
Russia
Tel: +7 495 787 28 13
Tel: +7 495 787 27 00
Tel: +7 495 787 31 84
Fax: +7 495 787 27 01
elena.kukushkina@bakermckenzie.com
georgy.mzhavanadze@bakermckenzie.com
vadim.perevalov@bakermckenzie.com
www.bakermckenzie.com

JUN HE LLP
China Resources Building
20th floor
8 Jianguomenbei Avenue
Beijing 100005
China
Tel: +86 10 8519 1718
Fax: +86 10 8519 1350
dongx@junhe.com
www.junhe.com

© 2017 Law Business Research Ltd
KOBYŁAŃSKA & LEWOSZEWSKI
KANCELARIA PRAWNA SP J
ul. Wspólna 50/11
00-684 Warsaw
Poland
Tel: +48 22 25 34567
Fax: +48 22 12 67142
anna.kobylnska@klattorneys.pl
marcin.lewoszewski@klattorneys.pl
www.klattorneys.pl

PERCHSTONE & GRAEYS
1 Perchstone & Graeys Close
off Remi Olowude
Lekki
Lagos
Nigeria
Tel: +234 1 342 9131
folabikuti@perchstoneandgraeys.com
ugochukwuobi@perchstoneandgraeys.com
sethazubuike@perchstoneandgraeys.com
www.perchstoneandgraeys.com

LEE & KO
Hanjin Building
63 Namdaemun-ro
Jung-gu
Seoul 04532
Korea
Tel: +82 2 772 4000
Fax: +82 2 772 4001
kwangbae.park@leeko.com
jubong.jang@leeko.com
www.leeko.com

SANTAMARINA Y STETA, SC
Ricardo Margain Zozaya 335
Tower I, floor 7
Valle del Campestre
66265 Garza García
Nuevo León
Mexico
Tel: +52 81 8133 6000/6002
Fax: +52 81 8368 0111
cruz@s-s.mx
dacosta@s-s.mx
www.s-s.mx

M&M BOMCHIL
Suipacha 268, 12th floor
Buenos Aires 1008
Argentina
Tel: +54 11 4321 7500
Fax: +54 11 4321 7555
adrian.furman@bomchil.com
francisco.zappa@bomchil.com
catalina.malara@bomchil.com
www.bomchil.com.ar

SIDLEY AUSTIN LLP
39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645
Fax: +852 2509 3110
yuetming.tham@sidley.com
Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3969
Fax: +65 6230 3939
yuetming.tham@sidley.com

NNOVATION LLP
World Exchange Plaza
45 O’Connor Street, Suite 1150
Ottawa
Ontario K1P 1A4
Canada
Tel: +1 613 656 1297
Fax: +1 888 314 5997
sbrown@nnovation.com
www.nnovation.com
Contributing Law Firms' Contact Details

Woolgate Exchange
25 Basinghall Street
EC2V 5HA
London
United Kingdom
Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
wlong@sidley.com
gscali@sidley.com
fblythe@sidley.com

1999 Avenue of the Stars, 17th floor
Los Angeles
California 90067
United States
Tel: +1 310 595 9500
Fax: +1 310 595 9501
ecooper@sidley.com
atutundjian@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com
ffaircloth@sidley.com

Sidley Austin Nishikawa Foreign Law
Joint Enterprise
Marunouchi Building 23F 4-1
Marunouchi 2-Chome
Chiyoda-ku
Tokyo 100-6323
Japan
Tel: +81 3 3218 5900
Fax: +81 3 3218 5922
tishiara@sidley.com

www.sidley.com

SIQUEIRA CASTRO – ADVOGADOS
Praça Pio X No. 15, 3rd floor
Centro
Rio de Janeiro 20040-020
Brazil
Tel: +55 21 2223 8818
Fax: +55 21 2516 8308
dpitanga@siqueiracastro.com.br
bg@siqueiracastro.com.br
www.siqueiracastro.com.br

SK CHAMBERS
9B Jalan Setiapuspa
Bukit Damansara
50490 Kuala Lumpur
Malaysia
Tel: +60 3 2011 6800
Fax: +60 3 2011 6801
sk@skchambers.co
www.skchambers.co

SUBRAMANIAM & ASSOCIATES
Central Square
Suite 328, Plaza III
20 Manoharlal Khurana Marg
Bara Hindu Rao (off Rani Jhansi Road)
Delhi 110 006
India
Tel: +91 11 30165700
Fax: +91 11 30165799
sna@sna-ip.com
www.sna-ip.com

URÍA MENÉNDEZ ABOGADOS, SLP
c/Príncipe de Vergara 187
Plaza de Rodrigo Uría
28002 Madrid
Spain
Tel: +34 915 860 131
Fax: +34 915 860 403
leticia.lopez-lapuente@uria.com
reyes.bermejo@uria.com
Contributing Law Firms' Contact Details

**VDA VIEIRA DE ALMEIDA**
Rua Dom Luis I 28
1200-109 Lisbon
Portugal
Tel: +351 21 311 3400
Fax: +351 213113406
mpc@vda.pt
iab@vda.pt
www.vda.pt

**WINHeller**
**Rechtsanwaltsgesellschaft mbH**
Tower 185
Friedrich-Ebert-Anlage 35–37
60327 Frankfurt am Main
Germany
Tel: +49 69 76 75 77 80
Fax: +49 69 76 75 77 810
info@winheller.com
www.winheller.com/en

**Walder Wyss Ltd**
Seefeldstrasse 123
PO Box 1236
8034 Zurich
Switzerland
Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
juerg.schneider@walderwyss.com
monique.sturny@walderwyss.com
hugh.reeves@walderwyss.com
www.walderwyss.com
www.dataprotection.ch

© 2017 Law Business Research Ltd