Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity

Keep the trust you've earned.

Complying with global privacy, data protection and cybersecurity rules is challenging, especially for businesses that operate across borders. Our top-ranked privacy team, in combination with the firm's Centre for Information Policy Leadership, advises on all aspects of US and European data protection law and cybersecurity events. We help businesses develop global compliance frameworks addressing regulatory obligations in the US, the EU and across the world. The firm is widely recognized globally as a leading privacy and data security firm.

For more information, visit www.huntonprivacyblog.com.

Publisher
Tom Barnes
tom.barnes@lbresearch.com

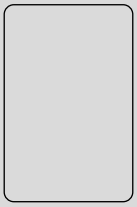
Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112



Data Protection & Privacy
2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction

Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

This introduction aims to highlight the main developments in the international privacy and data protection arena in the past year. The first introduction to this publication in 2012 noted the rapid growth of privacy and data protection laws across the globe and reflected on the commercial and social pressures giving rise to these global developments. Those economic and social pressures have not diminished since that first edition, and they are increasingly triggering new initiatives from legislators to regulate the use of personal information.

The exponential increase of privacy and data protection rules fuels the idea that personal information has become the new 'oil' of today's data-driven economies, with laws governing its use becoming ever more significant.

The same caveat as in previous editions still holds true today: as privacy and data protection rules are constantly evolving, any publication on the topic is likely to be outdated shortly after it is circulated. Therefore, anyone looking at a new project that involves the jurisdictions covered in this publication should verify whether there have been new legislative or regulatory developments since the date of writing.

Convergence of laws

In previous editions of this publication the variation in the types and content of privacy and data protection laws across jurisdictions has been highlighted. It has also been noted that, although privacy and data protection laws in different jurisdictions are far from identical, they often focus on similar principles and common themes.

Policymakers from various parts of the world have been advocating the need for 'convergence' between the different families of laws and international standards since the early days of privacy and data protection law. The thought was that, gradually, the different approaches would begin to coalesce, and that global standards on privacy and data protection would emerge over time. While there is little doubt that convergent approaches to privacy and data protection would benefit both businesses and consumers, it will be a long time before truly global privacy and data protection standards will become a reality.

Privacy and data protection rules are inevitably influenced by legal traditions, cultural and social values, and technological developments which differ from one part of the world to another. Global businesses should take this into consideration, especially if they are looking to introduce or change business processes across regions that involve the processing of personal information (for instance, about consumers or employees). Although it makes absolute sense for global businesses to implement common standards for privacy and data protection throughout their organisation, and regardless of where personal information is collected or further processed, there will always be differences in local laws that can have a significant impact on how personal information can be used.

International instruments

There are a number of international instruments that continue to have a significant influence on the development of privacy and data protection laws.

The main international instruments are:

- the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108+) of the Council of Europe;
- the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines);
- the European Union General Data Protection Regulation (GDPR);
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (the Framework); and
- the African Union Convention on Cyber Security and Personal Data Protection.

Convention 108 was originally adopted in 1981, but was modified in 2018 to more closely reflect data protection norms as they existed at that time. The newly adopted form is known as Convention 108+. Prior to its 2018 update, Convention 108 had been ratified by 53 countries; in June 2018, Cape Verde and Mexico became the fifth and sixth non-European countries, after Mauritius, Uruguay, Senegal and Tunisia, to ratify Convention 108. As of the date of publication, 35 countries have signed and three countries (Bulgaria, Croatia and Lithuania) have ratified the modified Convention 108+. Among other things, the modified Convention now includes genetic and biometric data as additional categories of sensitive data, a modernised approach to data subject rights (by recognising a right not to be subjected to automated decision making without the data subject's views being taken into account, and that individuals should be entitled to understand the underlying reasoning behind such processing), and explicitly requires signatories to clearly set forth the available legal bases for processing personal data. Convention 108+ also requires each party to establish an independent authority to ensure compliance with data protection principles and sets out rules on international data transfers. Convention 108+ is open to signature by any country and claims to be the only instrument providing binding standards with the potential to be applied globally. It has arguably become the backbone of data protection laws in Europe and beyond.

The OECD Guidelines are not subject to a formal process of adoption but were put in place by the Council of the OECD in 1980. Like Convention 108, the OECD Guidelines have been reviewed and revisions were agreed in July 2013. Where mostly European countries have acceded to Convention 108, the OECD covers a wider range of countries, including the US, which has accepted the Guidelines.

Although Convention 108 was recently updated, both Convention 108+ and the OECD Guidelines originally date from the 1980s. By the 1990s the EU was becoming increasingly concerned about divergences in data protection laws across EU member states and the possibility that intra-EU trade could be impacted by these divergences. The EU therefore passed Data Protection Directive 95/46/EC, which was implemented by the EU member states with a view to creating an EU-wide framework for harmonising data protection rules. Data Protection Directive 95/46/EC remained the EU's governing instrument for data protection until the GDPR came into force on 25 May 2018.

In 2004, these instruments were joined by a newer international instrument in the form of the APEC Privacy Framework, which was updated in 2015. Although it was subject to criticism when it was launched, the Framework has been influential in advancing the privacy debate in the Asia-Pacific region. The Framework aims to promote a flexible approach to privacy and data protection across the 21 APEC member economies while fostering cross-border flows of personal information. In November 2011, APEC leaders endorsed the Cross-Border Privacy Rules (CBPR) system, which is a voluntary accountability-based system to facilitate privacy-respecting flows of personal information among APEC economies. The APEC CBPR system is considered a counterpart to the European Union's system of binding corporate rules (BCRs) for data transfers outside of the EU. As of the date of publication, eight economies participate in the APEC CBPR system, including the United States, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, and Taiwan.

In June 2014, the African Union adopted a Convention on Cyber Security and Personal Data Protection as the first legal framework for cybersecurity and personal data protection on the African continent. Its goal is to address the need for harmonised legislation in the area of cybersecurity in member states of the African Union, and to establish in each member state mechanisms to combat privacy violations. So far the Convention has been signed by 14 African countries and ratified by five. It has been reported that a number of African countries have drafted data protection laws based on the Convention.

The European approach

For more than 20 years, data protection laws have been a salient feature of European legal systems. Each EU member state has introduced legislation based on Data Protection Directive 95/46/EC, which made it mandatory for member states to transpose the Directive's data protection principles into their national laws. In the same way, EU member state rules on electronic communications, marketing and the use of cookies follow the requirements of EU Directive 2002/58/EC on privacy and electronic communications.

The data protection laws of the EU's member states, the European Free Trade Association (Iceland, Liechtenstein and Norway) and EFTA-country Switzerland broadly follow the same pattern, since they were all based on or at least inspired by Data Protection Directive 95/46/EC. However, because Data Protection Directive 95/46/EC was not directly applicable, the laws adopted diverged in many areas. This has led to inconsistencies, which created complexity, legal uncertainty and additional costs for businesses that required to comply with, in many cases, 31 different data protection laws in Europe.

This was one the primary reasons why the European Commission introduced its EU Data Protection Reform in January 2012, which included the GDPR as well as a Data Protection Directive for the police and criminal justice sector (the Police and Criminal Justice Data Protection Directive). The GDPR establishes a single set of rules directly applicable throughout the EU, intended to streamline compliance for companies doing business in the EU. The European Commission estimated that the GDPR could lead to cost savings for businesses of around €2.3 billion a year.

After four years of negotiations, on 15 December 2015 the European Parliament, the Council of the EU and the European Commission reached a compromise on a new and arguably more harmonised data protection framework for the EU. The Council and the Parliament adopted the GDPR (EU 2016/679) and the Police and Criminal Justice Data Protection Directive (EU 2016/680) in April 2016, and the official texts were published the following month. While the GDPR entered into force on 24 May 2016, it became effective on 25 May 2018. The Police and Criminal Justice Data Protection Directive entered into force on 5 May 2016, and EU member states had until 6 May 2018 to transpose it into their national laws.

The GDPR has been a 'game changer' and one of the most significant developments in the history of EU and international data protection law. The impact of the GDPR is not confined to businesses based in the EU. The new rules apply to any processing of personal information conducted from outside the EU that involves the offering of goods or services to individuals in the EU or the monitoring of individuals in the EU.

As of the date of publication, all EU member states except Slovenia have enacted local data protection laws to supplement the GDPR in a range of areas (eg, sensitive data processing and data processing for employment purposes). However, these legislative initiatives at member state level are not aligned and therefore businesses find themselves – once again – in a situation where they have to comply with different member state laws in addition to the GDPR. Furthermore, almost all data protection authorities in the EU have published their own guidance and recommendations on how to comply with the GDPR, regardless of the guidelines that are being adopted at EU level (by representatives of the EU member state data protection authorities known as the Article 29 Working Party under the previous law). This variety of guidance and recommendations at EU and member state level has triggered confusion for businesses that are trying to determine how to comply with the GDPR.

In April 2016, the European Commission launched a public consultation on the review of the ePrivacy Directive. This review, which intended to pursue consistency between the ePrivacy Directive and the GDPR, raised questions about whether it is still necessary and meaningful to have separate rules on electronic privacy now that the GDPR has been adopted. Following the 2016 consultation, on 10 January 2017 the European Commission adopted a proposal for a Regulation on Privacy and Electronic Communications (the ePrivacy Regulation), which is intended to replace the ePrivacy Directive. The proposal was forwarded simultaneously to the European Parliament, the Council and member state parliaments, as well as to the Committee of the Regions and the Economic and Social Committee for review and adoption. The goal was to have the final text adopted by 25 May 2018, when the GDPR became applicable, but that goal was not achieved. At the time of drafting, there is still no definitive timeline on its adoption.

In addition to revamping the legal framework for general data protection, there has been an increased focus on cybersecurity in the EU. Since the adoption of its EU Cybersecurity Strategy in 2013, the European Commission has made laudable efforts to better protect Europeans online, which culminated in an action plan to further strengthen the EU's cyber resilience by establishing a contractual public-private partnership (PPP) with industry in July 2016. In addition, on 6 July 2016, the European Parliament adopted the Network and Information Security (NIS) Directive, which aims to protect 'critical infrastructure' in sectors such as energy, transport, banking and health, as well as key internet services. Businesses in these critical sectors will have to take additional security measures and notify serious data incidents to the relevant authorities. The NIS Directive entered into force in August 2016, but member states had until May 2018 to transpose the NIS Directive into their national laws.

Global perspective

United States and the EU

Moving outside Europe, the picture is more varied. From an EU perspective, the US is considered to have less regard for the importance of personal information protection. However, the US has had a Privacy Act regulating government departments and agencies since 1974, and many of the 50 states have their own privacy laws. Contrary to the EU's omnibus law approach, the US has historically adopted a sectoral approach to privacy and data protection. For instance, it has implemented specific privacy legislation aimed at protecting children online, the Children's Online Privacy Protection Act 1998 (COPPA). It has

also adopted specific privacy rules for health-related data, the Health Insurance Portability and Accountability Act (HIPAA). This approach is beginning to change, with the enactment in California of the nation's first comprehensive privacy, known as the California Consumer Privacy Act of 2018 (CCPA). The CCPA imposes obligations on a range of businesses to provide privacy notices, creates privacy rights of access, deletion and the opportunity to opt out of the sale of personal information, and imposes obligations on businesses to include specified language in their service provider agreements. Inspired by California, numerous other states are actively considering similarly comprehensive privacy legislation.

From a cybersecurity perspective, in October 2015, the US Senate passed the Cybersecurity Information Sharing Act (CISA), which aims to facilitate the sharing of information on cyber threats between private companies and US intelligence agencies. A few months later, the US Department of Homeland Security (DHS) issued guidelines and procedures for sharing information under the CISA. The Judicial Redress Act was enacted in February 2016 as a gesture to the EU that the US is taking privacy seriously. The Judicial Redress Act is designed to ensure that all EU citizens have the right to enforce data protection rights in US courts. In May 2017, President Trump signed an executive order aimed at strengthening the cybersecurity of federal networks and critical infrastructure.

The US also used to be in a privileged position on account of the EU–US Safe Harbor scheme, which had been recognised by the European Commission as providing adequate protection for the purposes of data transfers from the EU to the US. This formal finding of adequacy for companies that joined and complied with the Safe Harbor was heavily criticised in the EU following the Edward Snowden revelations. On 6 October 2015, in a landmark decision, the Court of Justice of the European Union (CJEU) declared the Safe Harbor invalid. This decision forced thousands of businesses that had relied directly or indirectly on the Safe Harbor to look for alternative ways of transferring personal information from the EU to the US. To address the legal vacuum that was created following the invalidation of the Safe Harbor, the European Commission and the United States agreed in February 2016 on a new framework for transatlantic data transfers: the EU–US Privacy Shield.

In accordance with the EU–US Privacy Shield adequacy decision that was adopted in July 2016, the first joint annual review of the Privacy Shield and how it functions in practice took place in September 2017. In its report concluding the first review, the European Commission reiterated its support for the Privacy Shield while outlining certain areas in need of improvement, including the need for ongoing monitoring of compliance with the Privacy Shield Principles by the Department of Commerce and strengthening of the privacy protections contained in the US Foreign Intelligence Surveillance Act (FISA). The Privacy Shield has also been subject to two further joint annual reviews in 2018 and 2019. In the European Commission's report following the latest review, the Commission welcomed further information provided by US authorities in relation to the Foreign Intelligence Surveillance Act, and highlighted a number of steps that should be taken to better ensure the effective functioning of the Privacy Shield (for example, by reducing the grace period that applies when organisations are required to recertify annually to a maximum period of 30 days).

Four years after the EU-US Privacy Shield was adopted, the CJEU invalidated the Privacy Shield on 16 July 2020. In a case known as *Schrems II* brought by Max Schrems – the privacy activist credited with initiating the downfall of Safe Harbor – the CJEU ruled that the EU-US Privacy Shield was not a valid mechanism to lawfully transfer EU personal data to the US. In the decision, the CJEU held that:

> *. . . the limitations on the protection of personal data arising from [US domestic law] on the access and use [of the transferred data] by US public authorities [. . .] are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.*

Further, the CJEU found that the EU-US Privacy Shield framework does not grant EU individuals actionable rights before a body offering guarantees that are substantially equivalent to those required under EU law. On those grounds, the CJEU declared the EU-US Privacy Shield invalid.

Asia-Pacific

In the Asia-Pacific region, the early adopters of privacy and data protection laws – Australia, New Zealand and Hong Kong SAR – have been joined by most of the other major jurisdictions. In early 2017, Australia amended its privacy act to introduce data breach notification requirements replacing the previous voluntary regime. China adopted a comprehensive Cybersecurity Law that came into effect on 1 June 2017. China's Cybersecurity Law contains a data localisation requirement applicable to operators of critical information infrastructure. A draft regulation would expand restrictions on cross-border data transfers to all network operators. The law also imposes personal information protection obligations (eg, notice and consent requirements) on network operators, in addition to a data breach notification requirement and obligations to implement cybersecurity protocols. Additional regulations and guidelines also are being considered in relation to the Cybersecurity Law, including draft guidelines concerning the security assessment of cross-border transfers of personal information and important data. Furthermore, on 1 May 2018, the Information Security Technology – Personal Information Security Specification (the Specification) came into effect in China, providing a best practice guide for the processing of personal information. While the Specification is not binding and cannot be used as a direct basis for enforcement, agencies in China can still use the Specification as a reference or guideline in their administration and enforcement activities.

In April 2018, the Hong Kong Privacy Commissioner for Personal Data announced plans to review and update the 1996 data protection law in light of the GDPR and recent large-scale data breaches affecting Hong Kong citizens' personal data.

In December 2016, Indonesia adopted its first data protection law, which focuses on the processing of personal information through electronic media.

Japan amended its Personal Information Protection Act in September 2015, creating an independent data protection authority and imposing restrictions on cross-border data transfers (which took effect in September 2017). On 17 July 2018, the EU and Japan successfully concluded negotiations on a reciprocal finding of an adequate level of data protection, thereby agreeing to recognise each other's data protection systems as 'equivalent'. This will allow personal data to flow legally between the EU and Japan, without being subject to any further safeguards or authorisations. The Personal Data Protection Standard in Malaysia came into force in December 2015 and complements the existing data protection law. The Malaysian data protection authority recently launched a public consultation on the rules regarding cross-border data transfers, which included an initial 'whitelist' of jurisdictions deemed adequate for overseas transfers. In the Philippines, the implementing rules for the Data Privacy Act of 2012 took effect in September 2016 and the law introduced GDPR-inspired concepts, such as a data protection officer designation and 72-hour breach notification requirements.

Having one of the most advanced data protection regimes in the region, Singapore passed its Cybersecurity Act in February 2018, which provides a national framework for the prevention and management of cyber incidents.

South Korea has lived up to its reputation as having one of the strictest data protection regimes in the Asia-Pacific region. The European Commission is actively engaging with South Korea regarding the possibility of recognising South Korean data protection law as equivalent and hence allowing unrestricted transfers of personal information to South Korea. In Taiwan amendments to the Personal Information Protection Act came into effect in March 2016. The amendments introduce, among other things, rules for processing sensitive personal information. Thailand adopted the Personal Data Protection Act in May 2019, with a one-year grace period until it will be enforced.

Finally, in December 2019, the Vietnamese Ministry of Public Security published a six-part draft Decree on Personal Data Protection, but as of the time of writing there is no clear indication of when the law will enter into force.

Central and South America

Latin America has seen a noticeable increase in legislative initiatives in recent years. Only a handful of Latin American countries currently do not have specific privacy and data protection laws. Argentina and Uruguay have modelled their data protection laws on the EU's approach under the EU Data Protection Directive, which explains why they are the only Latin American countries considered by the European Commission as providing an adequate level of data protection. In February 2017, Argentina initiated a revision process to align its data protection law with the GDPR, introducing concepts such as data portability and 72-hour breach reporting. Chile, Costa Rica, Panama and Peru have launched similar initiatives to Argentina's, while in January 2017 Mexico expanded the scope of its data protection law to cover data processing by private and public persons or entities. Nicaragua passed its data protection law in 2012, but it does not have a fully functioning data protection authority at this point. Other countries in Latin America have some degree of constitutional protection for privacy, including a right to habeas data, for example, in Brazil and Paraguay. On 10 July 2018, Brazil's Federal Senate approved a comprehensive data protection bill, known as the Brazilian General Data Protection Law (LGPD) that was inspired by the GDPR. The LGPD will be enforced from August 2020.

Africa

The global gaps in coverage lie in Africa and the Middle East. However, the number of countries with laws impacting personal information is steadily rising in both regions.

As noted earlier, the African Union adopted a Convention on Cyber Security and Personal Data Protection in June 2014. Initially there were concerns that the Convention was too vague and insufficiently focused on privacy rights. In May 2017, the Commission of the African Union and the Internet Society issued guidelines and recommendations to address these concerns.

An increasing number of African countries are implementing data protection laws as well as cybersecurity regulations irrespective of the Convention – currently, 24 out of 53 African countries have adopted laws and regulations that relate to the protection of personal data. Angola, for example, introduced its data protection law in 2011 and approved a law in 2016 that would create a data protection authority, although such an authority has not yet been established. Equatorial Guinea's new data protection law entered into force in August 2016, and is clearly inspired by EU data protection standards. Mauritania adopted data protection rules in June 2017, while South Africa passed a data protection law based on the (former) EU model in 2013, which is not fully in force yet but is expected to be fully effective by the end of 2020. In October 2015, the South African government created a virtual national cybersecurity hub to foster cooperation between the government and private companies. It also introduced a Cybercrimes and Cybersecurity Bill in December 2017, which as of the time of writing has not yet been enacted. Tanzania passed its Cyber Crime Act in September 2015, and in 2018 Benin updated its earlier 2009 legal framework on data protection, and Uganda is still in the process of preparing the adoption of its first privacy and data protection bill. Four African countries joined Convention 108 between 2016 and 2017: Cape Verde, Mauritius, Senegal and Tunisia. Mauritius also amended its data protection law in light of the EU GDPR, while Morocco published a Q&A in June 2017 on the possible impact of the GDPR on Moroccan companies.

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@huntonak.com

Lisa J Sotto
lsotto@huntonak.com

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772

200 Park Avenue
New York, NY 10166
Tel: +1 212 309 1000
Fax: +1 212 309 1100

www.huntonak.com

The Middle East

In the Middle East there are several laws that cover specific industry sectors but, apart from Israel, few countries have comprehensive data protection laws. Israel updated its data protection law in March 2017 by adding data security-related obligations, including data breach notification requirements. The European Commission recognises Israel as a jurisdiction that provides an adequate level of protection of personal data. Qatar passed its first data protection law in November 2016, which is largely inspired by the EU's data protection principles. In January 2018, the Dubai International Financial Centre Authority of the UAE amended its existing data protection law to bring it in line with the GDPR. The UAE's Abu Dhabi Global Market enacted similar amendments to its data protection regulations in February 2018.

Now more than ever, global businesses face the challenge of complying with a myriad of laws and regulations on privacy, data protection and cybersecurity. This can make it difficult to roll out new programmes, technologies and policies with a single, harmonised approach. In some countries, restrictions on cross-border data transfers will apply, while in others localisation requirements may require data to be kept in the country. In some jurisdictions, processing personal information generally requires individuals' consent, while in others consent should be used in exceptional situations only. Some countries have special rules on, for example, employee monitoring. Other countries rely on vague constitutional language.

This publication can hopefully continue to serve as a compass to those doing business globally and help them navigate the (increasingly) murky waters of privacy and data protection.

EU overview

Aaron P Simpson, Claire François and James Henderson
Hunton Andrews Kurth LLP

The EU General Data Protection Regulation (GDPR) became directly applicable in all EU member states from 25 May 2018 and in the European Economic Area European Free Trade Association member states (Iceland, Liechtenstein and Norway) in July 2018. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) dated 24 October 1995, and established a single set of rules throughout the EU, although EU member state data protection laws complement these rules in certain areas. The EU data protection authorities (DPAs) now gathered in the European Data Protection Board (EDPB) have published a number of guidelines on how to interpret and implement the new legal framework. This provides useful guidance to businesses on how to align their existing data protection practices with the GDPR.

Impact on businesses

The GDPR largely builds on the existing core principles of EU data protection law and expands them further while introducing new concepts that address the challenges of today's data-driven economy. In addition, the GDPR launches a new governance model that increases the enforcement powers of DPAs, enhances cooperation between them and promotes a consistent application of the new rules. The most significant concepts of the GDPR affecting businesses are outlined below.

Territorial scope

The GDPR is relevant to both EU businesses and non-EU businesses processing personal data of individuals in the EU. With regard to businesses established in the EU, the GDPR applies to all data processing activities carried out in the context of the activities of their EU establishments, regardless of whether the data processing takes place in or outside of the EU. The GDPR applies to non-EU businesses if they 'target' individuals in the EU by offering them products or services, or if they monitor the behaviour of individuals in the EU. Many online businesses that were previously not directly required to comply with EU data protection rules are now fully affected by the GDPR.

One-stop shop

One of the most important innovations introduced by the GDPR is the one-stop shop. The GDPR makes it possible for businesses with EU establishments to have their cross-border data protection issues handled by one DPA acting as a lead DPA. In addition to the lead DPA concept, the GDPR introduces the concept of a 'concerned' DPA to ensure that the lead DPA model will not prevent other relevant DPAs from having a say in how a matter is dealt with. The GDPR also introduces a detailed cooperation and consistency mechanism, in the context of which DPAs will exchange information, conduct joint investigations and coordinate enforcement actions. In case of a disagreement among DPAs with regard to possible enforcement action, the matter can be escalated to the European Data Protection Board (EDPB) for a final decision. Purely local complaints without a cross-border element can be handled by the concerned DPA at member state level, provided that the lead DPA has been informed and agrees to the proposed course of action. In some member states, such as France, businesses will have to approach the DPA they consider as their lead DPA by filing a specific form for the designation of the lead DPA.

Accountability

Under the GDPR, businesses are held accountable with regard to their data processing operations and compliance obligations, and the GDPR includes a general accountability principle that requires controllers to be able to demonstrate their compliance with the GDPR's obligations. The GDPR also imposes a number of specific obligations on data controllers and data processors in this respect. Data controllers are required to implement and update – where necessary – appropriate technical and organisational measures to ensure that their data processing activities are carried out in compliance with the GDPR, and to document these measures to demonstrate such compliance at any time. This includes the obligation to apply the EU data protection principles at an early stage of product development and by default (privacy by design/default). It also includes the implementation of various compliance tools to be adjusted depending on the risks presented by the data processing activities for the privacy rights of individuals. Data protection impact assessments (DPIAs) are such tools, which will have to be conducted in cases of high-risk data processing, and certain other specified processing activities, such as those that involve processing of sensitive data on a large scale. Data processors are required to assist data controllers in ensuring compliance with their accountability obligations, including DPIAs, the implementation of appropriate security measures, and the handling of data subject rights requests. In addition, data controllers and data processors have to implement robust data security measures and keep internal records of their data processing activities, a system that replaces the previous requirement to register with the DPAs at member state level. Furthermore, in some cases, data controllers and data processors are required to appoint a data protection officer (DPO), for example, if their core activities involve regular and systematic monitoring of individuals or the processing of sensitive data on a large scale. The accountability obligations of the GDPR therefore require businesses to have comprehensive data protection compliance programmes in place.

Data breach notification

The GDPR introduces a general data breach notification requirement applicable to all industries. All data controllers now have to notify data breaches to the DPAs without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Delayed notifications must be accompanied by a reasoned justification and the information related to the breach can be provided in phases. In addition, data controllers have to notify affected individuals if the breach is likely to result in a high risk to the individuals' rights and freedoms. Businesses face the challenge of developing data breach response plans and taking other breach readiness measures to avoid fines and the

negative publicity associated with data breaches. Data processors are required to notify data controllers of personal data breaches, but do not have an independent obligation to notify DPAs or affected individuals.

Data processing agreements

The GDPR imposes minimum language that needs to be included in agreements with service providers acting as data processors. The GDPR requires, for example, that data processing agreements include documented instructions from the data controller regarding the processing and transfer of personal data to third countries (ie, outside of the EU), a requirement for the processor to implement appropriate data security measures, the possibility for the data controller (or a third party mandated by the data controller) to carry out audits and inspections, and an obligation to delete or return personal data to the data controller upon termination of the services. The new requirements for data processing agreements under the GDPR require many businesses to review and renegotiate existing vendor and outsourcing agreements. The EDPB and some DPAs (such as the French and Spanish DPAs) have developed template clauses to help businesses ensure compliance with those requirements.

Consent

Under the GDPR, consent must be based on a clear affirmative action and be freely given, specific, informed and unambiguous. Consent language hidden in terms and conditions, pre-ticked boxes or inferred from silence is not valid. Also, consent is unlikely to be valid where there is a clear imbalance of power between the individual and the data controller seeking the consent, such as in employment matters. Electronic consent is acceptable, but it has to be clear, concise and not unnecessarily disruptive. In the context of a service, the provision of the service should not be made conditional on customers consenting to the processing of personal data that is not necessary for the service. Further, the GDPR requires data controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent. Given the stringent consent regime in the GDPR, businesses relying on consent for their core activities should carefully review their consent practices.

Transparency

Under the GDPR, privacy notices must be provided in a concise, transparent, intelligible and easily accessible form to enhance transparency for individuals. In addition to the information that privacy notices already had to include under the previous regime, the GDPR requires that privacy notices specify the contact details of the DPO (if any), the legal basis for the processing, any legitimate interests pursued by the data controller or a third party (where the data controller relies on such interests as a legal basis for the processing), the controller's data retention practices, how individuals can obtain a copy of the data transfer mechanisms that have been implemented, and whether personal data is used for profiling purposes. When personal data is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the personal data originated and the categories of personal data obtained. In light of the volume of the information required, DPAs recommend adopting a layered approach to the provision of information to individuals (such as the use of a layered privacy notice in a digital context). These new transparency requirements require businesses to review their privacy notices.

Rights of individuals

The GDPR strengthens the existing rights of individuals and introduces additional rights. For instance, the GDPR strengthens the right of individuals to object to the processing of their personal data. In addition, the GDPR enhances the right to have personal data erased by introducing a 'right to be forgotten'. This right applies when personal data is no longer necessary or, more generally, where the processing of personal data does not comply with or no longer complies with the GDPR. Furthermore, the GDPR introduces the right to data portability, based on which individuals can request to have their personal data returned to them or transmitted to another data controller in a structured, commonly used and machine-readable format. The right to data portability applies only with regard to automated processing based on consent or processing that is necessary for the performance of a contract. Businesses need to review their existing practices for handling individuals' requests and consider how to give effect to the new rights of individuals under the GDPR. Individuals may also have a right to restrict the processing of personal data in some circumstances, such as while the accuracy of personal data is verified by the data controller. When processing of personal data is restricted, the data controller may only:

- store the data;
- process the data to establish or exercise legal claims;
- protect the rights of another natural or legal person;
- process the personal data for reasons of public interest; or
- process the personal data for other purposes with the data subject's consent.

Data transfers

The GDPR maintains the general prohibition of data transfers to countries outside of the EU that do not provide an 'adequate' level of data protection, and applies stricter conditions for obtaining an 'adequate' status. The GDPR introduces alternative tools for transferring personal data outside of the EU, such as codes of conduct and certification mechanisms, although none have been approved by regulators to date. The previous contractual options for data transfers have been expanded and made easier; going forward, regulators may also adopt standard contractual clauses to be approved by the European Commission, and it is now no longer required to obtain the DPAs' prior authorisation for transferring personal data outside of the EU and submit copies of executed standard contractual clauses (which was previously required in some member states). In addition, the GDPR formally recognises binding corporate rules (BCRs) – internal codes of conduct used by businesses to transfer personal data to group members outside of the EU – as a valid data transfer mechanism for both data controllers and data processors. That said, as a result of the *Schrems II* decision, the EU-US Privacy Shield Framework is no longer a valid mechanism for transferring personal data to the US. Organisations that rely on standard contractual clauses (and other transfer mechanisms, such as BCRs) must now assess each data transfer on a case-by-case basis to determine whether there is an adequate level of protection for personal data that is to be transferred outside of the EU.

Administrative fines and right of individuals to effective judicial remedy

In the previous regime, some DPAs (such as the Belgian DPA) did not have the power to impose administrative fines. The GDPR gives this power to all DPAs and introduces high administrative fines that will significantly change the currently fragmented enforcement landscape. Member state DPAs may now impose administrative fines of up to the greater of €10 million or 2 per cent of a company's total worldwide annual turnover, or the greater of €20 million or 4 per cent of a company's total worldwide annual turn-over, depending on the nature of the violation. In addition, the GDPR expressly enables individuals to bring proceedings against data controllers and data processors, in particular to obtain compensation for damage suffered as a result of a violation of the GDPR.

The WP29 's and EDPB GDPR guidance

The Article 29 Working Party (WP29), composed of representatives of DPAs, has ceased to exist and was replaced by the EDPB as of 25 May 2018. During its first plenary meeting on 25 May 2018, the EDPB endorsed all the GDPR guidelines adopted by the WP29. In total, the WP29 adopted 16 GDPR guidelines and related documents clarifying key concepts and new requirements of the GDPR, including:

- guidelines on the right to data portability;
- guidelines on DPOs;
- guidelines for identifying a data controller or processor's lead DPA;
- guidelines on DPIA and determining whether processing is likely to result in a high risk to the individuals' rights and freedoms;
- guidelines on automated individual decision-making and profiling;
- guidelines on data breach notifications;
- guidelines on administrative fines;
- BCR referential for data controllers;
- BCR referential for data processors;
- adequacy referential;
- guidelines on transparency;
- guidelines on consent;
- updated working document on BCR approval procedure;
- revised BCR application form for controller BCRs;
- revised BCR application form for processor BCRs; and
- position paper on the derogations from the obligation to maintain internal records of processing activities.

In addition, the EDPB also has adopted guidelines that relate to the following:

- consent under the GDPR;
- processing of personal data through video devices;
- processing in the context of the provision of online services to data subjects;
- accreditation of certification bodies under article 43;
- territorial scope;
- derogations from the prohibition on data transfers;
- the use of location data and contact tracing tools, in the context of the covid-19 outbreak; and
- processing of data concerning health for the purpose of scientific research, in the context of the covid-19 outbreak.

EU member state complementing laws

Although the main objective of the GDPR is to harmonise data protection law across the EU, EU member states can and have introduced additional or more specific rules in certain areas; for example, if processing involves health data, genetic data, biometric data, employee data or national identification numbers, or if processing personal data serves archiving, scientific, historical research or statistical purposes. In addition, EU member state laws may require the appointment of a DPO in cases other than those listed in the GDPR. The German Federal Data Protection Act of 30 June 2017, for example, requires businesses to appoint a DPO if they permanently engage at least 10 persons in the data processing, if they carry out data processing activities subject to a DPIA, or if they commercially process personal data for market research purposes. EU member states may also provide for rules regarding the processing of personal data of deceased persons. The French Data Protection Act, as updated on June 21 2018, for example, includes such rules by granting individuals the right to define the way their personal data will be processed after their death, in addition to the GDPR rights. In the context of online services directed to children, the GDPR requires parental consent for children below the age of 16, but EU member state law may prescribe a lower age limit, provided it is not lower than the age of 13. This limit is lowered to the age of 13, for example, in the UK Data Protection Act 2018 and the age of 14 in the Austrian Data Protection Amendment Act 2018. At the time of writing, all EU member states other than Slovenia have adopted their new national data protection laws. This creates additional layers of complexity for businesses, which should closely monitor these developments in the relevant member states and assess the territorial scope of the specific national rules, where applicable.

In summary, it is fair to say that the GDPR has created a more robust and mature data protection framework in the EU, while EU member state laws complement that framework. The new rules affect virtually any business dealing with personal data relating to individuals in the EU. Businesses should at the very least be able to demonstrate that they have engaged in a GDPR compliance programme, in light of the enhanced enforcement powers available to DPAs under the GDPR and the increasing focus on data protection issues since the GDPR entered into effect.

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@huntonak.com

Claire François
cfrancois@huntonak.com

James Henderson
jhenderson@huntonak.com

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
Tel: +32 2 643 58 00
Fax: +32 2 643 58 22

www.huntonak.com

The Privacy Shield

Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Twenty-first century commerce depends on the unencumbered flow of data around the globe. At the same time, however, individuals are clamouring for governments to do more to safeguard their personal data. A prominent outgrowth of this global cacophony has been reinvigorated regulatory focus on cross-border data transfers. Russia made headlines because it enacted a law in 2015 that requires companies to store the personal data of Russians on servers in Russia. While this is an extreme example of 'data localisation', Russia is not alone in its effort to create impediments to the free flow of data across borders. The Safe Harbor framework, which was a popular tool used to facilitate data flows from the European Union to the United States for nearly 15 years, was invalidated by the Court of Justice of the European Union (CJEU) in 2015, in part as a result of the PRISM scandal that arose in the wake of Edward Snowden's 2013 revelations. The invalidation of Safe Harbor raised challenging questions regarding the future of transatlantic data flows. A successor framework, the EU–US Privacy Shield, was unveiled by the European Commission in February 2016 and was formally approved in Europe in July 2016. In 2017, the Swiss government announced its approval of a Swiss–US Privacy Shield framework. On 16 July 2020, four years after the EU–US Privacy Shield was formally approved, it was invalidated by the CJEU, again as a result of concerns arising from the US surveillance framework. The CJEU's decision to invalidate the EU-US Privacy Shield has left Privacy Shield-certified organisations scrambling to identify and implement alternative data transfer mechanisms to lawfully transfer EU personal data to the US.

Contrasting approaches to privacy regulation in the EU and US

Privacy regulation tends to differ from country to country, as it represents a culturally bound window into a nation's attitudes about the appropriate use of information, whether by government or private industry. This is certainly true of the approaches to privacy regulation taken in the EU and the US, which historically have been both literally and figuratively an ocean apart. Policymakers in the EU and the US were able to set aside these differences in 2000 when they created the Safe Harbor framework, which was developed explicitly to bridge the gap between the differing regulatory approaches taken in the EU and the US. With the onset of the Privacy Shield, policymakers again sought to bridge the gap between the different regulatory approaches in the EU and US.

The European approach to data protection regulation

Largely as a result of the role of data accumulation and misuse in the human rights atrocities perpetrated in mid-20th-century Europe, the region has a hard-line approach to data protection. The processing of personal data about individuals in the EU is strictly regulated on a pan-EU basis by the General Data Protection Regulation (GDPR). Unlike its predecessor, the Data Protection Directive 95/46/EC, the GDPR is not implemented differently at the member state level but applies directly across the EU.

Extraterritorial considerations are an important component of the data protection regulatory scheme in Europe, as policymakers have no interest in allowing companies to circumvent European data protection regulations simply by transferring personal data outside of Europe. These extraterritorial restrictions are triggered when personal data is exported from Europe to the vast majority of jurisdictions around the world that have not been deemed adequate by the European Commission; chief among them from a global commerce perspective is the United States.

The US approach to privacy regulation

Unlike Europe, and for its own cultural and historical reasons, the US does not maintain a singular, comprehensive data protection law regulating the processing of personal data. Although it is beginning to change with the onset of more comprehensive laws at the state level such as the California Consumer Privacy Act, the US generally favours a sectoral approach to privacy regulation. As a result, in the US there are numerous privacy laws that operate at the federal and state levels, and they further differ depending on the industry within the scope of the law. The financial services industry, for example, is regulated by the Gramm-Leach-Bliley Act, while the healthcare industry is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Issues that fall outside the purview of specific statutes and regulations are subject to general consumer protection regulation at the federal and state level. Making matters more complicated, common law in the US allows courts to play an important quasi-regulatory role in holding businesses and governments accountable for privacy and data security missteps.

The development of the Privacy Shield framework

As globalisation ensued at an exponential pace during the internet boom of the 1990s, the differences in the regulatory approaches favoured in Europe versus the US became a significant issue for global commerce. Massive data flows between Europe and the US were (and continue to be) relied upon by multinationals, and European data transfer restrictions threatened to halt those transfers. Instead of allowing this to happen, in 2000 the European Commission and the US Department of Commerce jointly developed the Safe Harbor framework.

The Safe Harbor framework was an agreement between the European Commission and the US Department of Commerce whereby data transfers from Europe to the US made pursuant to the accord were considered adequate under European law. Previously, in order to achieve the adequacy protection provided by the framework, data importers in the US were required to make specific and actionable public representations regarding the processing of personal data they imported from Europe. In particular, US importers had to comply with the seven Safe Harbor principles of notice, choice, onward transfer, security, access, integrity and enforcement. Not only did US importers have to comply with these principles, they also had to publicly certify their compliance with the US Department of Commerce and thus subject themselves to enforcement by the US Federal Trade Commission (FTC) to the extent their certification materially misrepresented any aspect of their processing of personal data imported from Europe.

From its inception, Safe Harbor was popular with a wide variety of US companies that had operations involving the importing of personal data from Europe. While many of the companies that certified to the framework in the US did so to facilitate intracompany transfers of employee and customer data from Europe to the US, there are a wide variety of others who certified for different reasons. Many of these include third-party IT vendors with business operations that called for the storage of client data in the US, including personal data regarding a client's customers and employees. In the years immediately following the inception of the Safe Harbor framework, a company's participation in the Safe Harbor framework in general went largely unnoticed outside the privacy community. However, recently that relative anonymity changed, as the Safe Harbor framework faced an increasing amount of pressure from critics in Europe and, ultimately, was invalidated in 2015.

Invalidation of the Safe Harbor framework

Criticism of the Safe Harbor framework from Europe began in earnest in 2010. In large part, the criticism stemmed from the perception that the Safe Harbor was too permissive of third-party access to personal data in the US, including access by the US government. The *Düsseldorfer Kreises*, the group of German state data protection authorities, first voiced these concerns and issued a resolution in 2010 requiring German exporters of data to the US through the framework to employ extra precautions when engaging in such data transfers.

After the *Düsseldorfer Kreises* expressed its concerns, the pressure intensified and spread beyond Germany to the highest levels of government across Europe. This pressure intensified in the wake of the PRISM scandal in the summer of 2013, when Edward Snowden alleged that the US government was secretly obtaining individuals' (including EU residents') electronic communications from numerous online service providers. Following these explosive allegations, regulatory focus in Europe shifted in part to the Safe Harbor framework, which was blamed in some circles for facilitating the US government's access to personal data exported from the EU.

As a practical matter, in the summer of 2013, the European Parliament asked the European Commission to examine the Safe Harbor framework closely. In autumn 2013, the European Commission published the results of this investigation, concluding that the framework lacked transparency and calling for its revision. In particular, the European Commission recommended more robust enforcement of the framework in the US and more clarity regarding US government access to personal data exported from the EU under the Safe Harbor framework.

In October 2015, Safe Harbor was invalided by the CJEU in a highly publicised case brought by an Austrian privacy advocate who challenged the Irish Data Protection Commissioner's assertion that the Safe Harbor agreement precludes the Irish agency from stopping the data transfers of a US company certified to the Safe Harbor from Ireland to the US. In its decision regarding the authority of the Irish Data Protection Commissioner, the CJEU assessed the validity of the Safe Harbor adequacy decision and held it invalid. The CJEU's decision was based, in large part, on the collection of personal data by US government authorities. For example, the CJEU stated that the Safe Harbor framework did not restrict the US government's ability to collect and use personal data or grant individuals sufficient legal remedies when their personal data was collected by the US government.

The Privacy Shield

Following the invalidation of Safe Harbor, the European Commission and US Department of Commerce negotiated and released a successor framework, the EU–US Privacy Shield, in February 2016. Both the EU–US and Swiss–US Privacy Shield frameworks (collectively, the Privacy Shield) were approved by the European Commission and the Swiss government, respectively. The Privacy Shield is similar to Safe Harbor and contains seven privacy principles to which US companies may publicly certify their compliance. Prior to the invalidation of the EU-US Privacy Shield on 16 July 2020, after certification, entities certified as compliant with the Privacy Shield could import personal data from the EU without the need for another cross-border data transfer mechanism, such as standard contractual clauses. The Swiss-US Privacy Shield similarly permits certified organisations to import personal data from Switzerland without the need for another transfer mechanism. The privacy principles in the Privacy Shield are substantively comparable to those in Safe Harbor, but are more robust and more explicit with respect to the actions an organisation must take in order to comply with the principles. In developing the Privacy Shield principles and accompanying framework, policymakers attempted to respond to the shortcomings of the Safe Harbor privacy principles and framework identified by the CJEU.

After releasing the Privacy Shield, some regulators and authorities in Europe (including the former Article 29 Working Party (WP29), the European Parliament and the European Data Protection Supervisor) criticised certain aspects of the Privacy Shield as insufficient to protect personal data. For example, the lack of clear rules regarding data retention was heavily criticised. In response to these criticisms, policymakers negotiated revisions to the Privacy Shield framework to address the shortcomings and increase its odds of approval in Europe. Based on this feedback, the revised Privacy Shield framework was released in July 2016 and formally approved in the European Union. In addition, WP29, which previously was the group of European Union member state data protection authorities, subsequently offered its support, albeit tepid, for the new framework.

First annual review

Under the renegotiated framework, Privacy Shield was subject to annual reviews by the European Commission to ensure it functioned as intended. In September 2017, the US Department of Commerce and the European Commission conducted the first annual joint review of the Privacy Shield, focusing on any perceived weaknesses of the Privacy Shield, including with respect to government access requests for national security reasons, and how Privacy Privacy Shield-certified entities sought to comply with their Privacy Shield obligations. In November 2017, WP29 adopted an opinion on the review. The opinion noted that WP29 'welcomes the various efforts made by US authorities to set up a comprehensive procedural framework to support the operation of the Privacy Shield'. The opinion also identified some remaining concerns and recommendations with respect to both the commercial and national security aspects of the Privacy Shield framework. The opinion indicated that, if the EU and US did not, within specified time-frames, adequately address WP29's concerns about the Privacy Shield, WP29 might bring legal action to challenge the Privacy Shield's validity.

In March 2018, the US Department of Commerce provided an update summarising actions the agency had taken between January 2017 and March 2018 to support the EU–US and EU–US Privacy Shield frameworks. These measures addressed both commercial and national security issues associated with the Privacy Shield. With respect to the Privacy Shield's commercial aspects, the US Department of Commerce highlighted:

- an enhanced certification process, including more rigorous company reviews and reduced opportunities for false claims regarding Privacy Shield certification;
- additional monitoring of companies through expanded compliance reviews and proactive checks for false claims;
- active complaint resolution through the confirmation of a full list of arbitrators to support EU individuals' recourse to arbitration;
- strengthened enforcement through continued oversight by the FTC, which announced three Privacy Shield-related false claims actions in September 2017; and

- expanded outreach and education, including reaffirmation of the framework by federal officials and educational outreach to individuals, businesses and authorities.

With respect to national security, the US Department of Commerce noted measures taken to ensure:

- robust limitations and safeguards, including a reaffirmation by the intelligence community of its commitment to civil liberties, privacy and transparency through the updating and re-issuing of Intelligence Community Directive 107;
- independent oversight through the nomination of three individuals to the US Privacy and Civil Liberties Oversight Board (PCLOB) with the aim of restoring the independent agency to quorum status;
- individual redress through the creation of the Privacy Shield Ombudsperson mechanism, which provides EU and Swiss individuals with an independent review channel in relation to the transfer of their data to the US; and
- US legal developments take into account the Privacy Shield, such as Congress's reauthorisation of the Foreign Intelligence Surveillance Act's Section 702 (reauthorising elements on which the European Commission's Privacy Shield adequacy determination was based) and enhanced advisory and oversight functions of the PCLOB.

In June 2018, the debate regarding the Privacy Shield resurfaced when the Civil Liberties Committee of the European Parliament (LIBE) voted on a resolution to recommend that the European Commission suspend the Privacy Shield unless the US complied fully with the framework by 1 September 2018. This resolution, which passed by a vote of the full European Parliament on 5 July 2018, was a non-binding recommendation. Notwithstanding the result of the full vote, the Privacy Shield was not suspended at that time and continued with the Privacy Shield Principles unchanged.

Second annual review

In October 2018, the US Department of Commerce and the European Commission conducted the second annual review of the Privacy Shield, focusing on all aspects of Privacy Shield functionality. The review found significant growth in the program since the first annual review and noted several key points, including:

- more than 4,000 companies certified to the Privacy Shield since the framework's inception, and the US Department of Commerce's promise to revoke the certification of companies that do not comply with the Privacy Shield's principles;
- the appointment of three new members to the PCLOB by the US, and the PCLOB's declassification of its report on a presidential directive that extended certain signals intelligence privacy protections to foreign citizens;
- the ongoing review of the Privacy Shield Ombudsperson Mechanism, and the need for the US to promptly appoint a permanent under secretary; and
- recent privacy incidents affecting both US and EU residents reaffirming the 'need for strong privacy enforcement to protect our citizens and ensure trust in the digital economy'.

The European Commission's December 2018 publication of its report on the second annual review (the 2018 Commission Report) furthered several of these points. The 2018 Commission Report concluded that the US continued to ensure an adequate level of protection was given to personal data transferred from the EU to US companies under the EU–US Privacy Shield. The 2018 Commission Report also found that US authorities took measures to implement the Commission's recommendations from the previous year and several aspects of the functioning of the framework had improved. It also noted, however, several areas of concern, including companies' false claims of participation in and other examples of non-compliance with the Privacy Shield, lack of clarity in Privacy Shield guidance developed by the US Department of Commerce and European Data Protection Authorities, and delayed appointment and uncertain effectiveness of a permanent privacy shield ombudsman.

Subsequently, in January 2019, the European Data Protection Board (EDPB) also issued a report on the second annual review (the 2019 EDPB Report). Although not binding on EU or US authorities, the 2019 EDPB Report provided guidance to regulators in both jurisdictions regarding implementation of the Privacy Shield and highlighted the EDPB's ongoing concerns with regard to the Privacy Shield. The 2019 EDPB Report praised certain actions and efforts undertaken by US authorities and the European Commission to implement the Privacy Shield, including:

- efforts by the US Department of Commerce to adapt the certification process to minimise inaccurate or false claims of participation in the Privacy Shield;
- enforcement actions and other oversight measures taken by the US Department of Commerce and FTC regarding Privacy Shield compliance; and
- issuance of guidance for EU individuals on exercising their rights under the Privacy Shield, and for US businesses to clarify the requirements of the Privacy Shield.

The 2019 EDPB Report also raised similar concerns regarding the United States' ability to:

- oversee and enforce compliance with all Privacy Shield principles (particularly the onward transfer principle);
- delay in the appointment of a permanent privacy shield ombudsman;
- lack of clarity in guidance and conflicting interpretations of various topics, such as the definition of HR data; and
- shortcomings of the re-certification process, which, according to the 2019 EDPB Report, leads to an outdated listing of Privacy Shield-certified companies and confusion for data subjects.

Third annual review

On 23 October 2019, the European Commission published its report on the third annual review of the Privacy Shield. The report confirmed that the US continued to provide an adequate level of protection for personal data transferred pursuant to the Privacy Shield and noted several improvements made to the Privacy Shield framework following the second annual review. These improvements included efforts by US authorities to monitor participants' compliance with the Privacy Shield framework and the appointment of Keith Krach, Under Secretary of State for Economic Growth, Energy and the Environment, to the position of Privacy Shield Ombudsperson on a permanent basis (the vacancy of this position had been flagged in the two previous annual reviews). The European Commission's report on the third annual review noted that the number of Privacy Privacy Shield-certified organisations exceeded 5,000 at the time of the report, surpassing the number of companies that had previously registered for the now-defunct Safe Harbor framework in the nearly 15 years that Safe Harbor operated.

In its report on the third annual review, the European Commission also made the following findings and recommendations:

- The European Commission recommended shortening the 'recertification grace period' from the 3.5 months currently permitted by the Department of Commerce to a maximum of 30 days. The European Commission also recommended that the Department of Commerce send warning letters to companies that fail to recertify within 30 days of their recertification deadline.
- The European Commission recommended that the Department of Commerce strengthen its efforts to identify companies that have never certified to the Privacy Shield but nevertheless falsely claim

to be certified, noting that the Department of Commerce's verification efforts appear to have been focused on checking whether companies continue to claim Privacy Shield participation even after their certifications had lapsed.

- With respect to enforcement, the European Commission praised the FTC for bringing enforcement actions for violations of the Privacy Shield, but recommended that the FTC ensure it can share 'meaningful Information on ongoing investigations' with the European Commission and European data protection authorities.
- The European Commission recommended that data protection authorities continue to refine the definition of what falls within human resources data, given differing interpretations of the term by the various authorities and the lack of clear joint guidance.

Applicability of the Privacy Shield after Brexit

On 20 December 2018, the US Department of Commerce updated its frequently asked questions (FAQs) on the EU–US and EU–US Privacy Shield Frameworks to clarify the effect of the United Kingdom's planned withdrawal from the European Union (Brexit). The FAQs provided information on the steps Privacy Shield participants would need to take to receive personal data from the UK in reliance on the Privacy Shield after Brexit. This included requirements for Privacy Shield-certified organisations to implement certain changes to their public-facing Privacy Shield representations to expressly state their commitment to apply the Privacy Shield Principles to UK personal data received in the US in reliance on the Privacy Shield. Pursuant to the Withdrawal Agreement implementing the UK's departure from the EU, EU law (including EU data protection law) continues to apply in the UK during a Transition Period of 31 January 2020 to 31 December 2020. During the Transition Period, the European Commission's decision on the adequacy of the protection for personal data provided by the Privacy Shield was to apply to transfers of personal data from the UK to Privacy Shield participants in the US. As a result of the end of the Transition Period being set for 31 December 2020, in these FAQs, the Department of Commerce had set a deadline of 31 December 2020 to implement these required changes in order for the Privacy Shield to serve as a mechanism to transfer UK personal data to the US lawfully. In addition, the FAQs further stated that if a Privacy Shield participant opted to make such public commitments to continue receiving UK personal data in reliance on the Privacy Shield, the participant would be required to cooperate and comply with the UK Information Commissioner's Office with regard to any such personal data received.

As described in further detail below, the EU-US Privacy Shield was invalidated by the CJEU on 16 July 2020. As of the date of this writing, the Privacy Shield is no longer a lawful data transfer mechanism with respect to UK personal data, regardless of the Transition Period, and the Department of Commerce has not updated its UK-specific FAQs to discuss the impact of the invalidation specifically on the previously released requirements for Privacy Shield-certified organisations. Given the Department of Commerce's stated intention to continue administration and enforcement of the Privacy Shield, to understand their obligations going forward, organisations must keep a careful eye on developments related to the overlapping impacts of the UK's withdrawal from the EU and the CJEU's decision to invalidate the Privacy Shield.

US Privacy Shield enforcement actions

The FTC brought numerous enforcement actions against companies for false claims of participation in and non-compliance with the Privacy Shield. In September 2018, the FTC announced settlement agreements with four companies – IDmission LLC (IDmission); mResource LLC, doing business as Loop Works LLC (mResource); SmartStart Employment Screening Inc (SmartStart); and VenPath Inc (VenPath) – over allegations that each company had falsely claimed to have valid certifications under the EU–US Privacy Shield framework. The FTC alleged that SmartStart, VenPath and mResource continued to post statements on their websites about their participation in the Privacy Shield after allowing their certifications to lapse. IDmission had applied for a Privacy Shield certification but never completed the necessary steps to be certified. In addition, the FTC alleged that both VenPath and SmartStart failed to comply with a provision under the Privacy Shield requiring companies that cease participation in the Privacy Shield framework to affirm to the US Department of Commerce that they will continue to apply the Privacy Shield protections to personal information collected while participating in the program. As part of the FTC settlements, each company is prohibited from misrepresenting its participation in any privacy or data security program sponsored by the government or any self-regulatory or standard-setting organisation and must comply with FTC reporting requirements. Further, VenPath and SmartStart must either continue to apply the Privacy Shield protections to personal information collected while participating in the Privacy Shield, protect it by another means authorised by the Privacy Shield framework, or return or delete the information within 10 days of the FTC's order.

Similarly, on 14 June 2019, the FTC announced a proposed settlement with the Florida-based background screening company, SecurTest Inc, over allegations that SecurTest started, but did not complete, an application to certify to the Privacy Shield and nevertheless represented that it was Privacy Shield certified. The proposed settlement would prohibit SecurTest from misrepresenting the extent to which it is a member of any self-regulatory framework, including the Privacy Shield. That same month, the FTC announced it had sent warning letters to 13 US companies for falsely claiming participation in the now-defunct Safe Harbor Framework. In a press release, the FTC stated that it called on the 13 companies to remove from their websites, privacy policies, or any other public documents any statements claiming participation in Safe Harbor. The FTC noted that it would take legal action if the companies failed to remove such representations within 30 days. Taken together, the recent increase in FTC enforcement of the Privacy Shield demonstrates the agency's commitment to oversee and enforce compliance with the framework's principles.

Between November 2019 and January 2020, the FTC brought an additional 10 enforcement actions against companies alleged to have violated the Privacy Shield by falsely claiming to be certified to the framework. In November 2019, the FTC announced a settlement with Medable Inc stemming from allegations that, although Medable did initiate an application with the Department of Commerce in December 2017, the company never completed the steps necessary to participate in the framework. Then, in December 2019, the FTC announced settlements in four separate Privacy Shield cases. Specifically, the FTC alleged that Click Labs Inc, Incentive Services, Inc, Global Data Vault LLC and TDARX Inc each falsely claimed to participate in the EU–US Privacy Shield framework. The FTC also alleged that Click Labs and Incentive Services falsely claimed to participate in the EU–US Privacy Shield framework and that Global Data and TDARX continued to claim participation in the EU–US Privacy Shield after their Privacy Shield certifications lapsed. The complaints further alleged that Global Data and TDARX failed to comply with the Privacy Shield framework, including by failing to verify annually that statements about their Privacy Shield practices were accurate, and affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the program.

The following month, in January 2020, the FTC announced an additional five Privacy Shield settlements. The FTC had alleged, in separate actions, that DCR Workforce Inc, Thru Inc, LotaData Inc and 214 Technologies Inc had made false claims on their websites that they were certified under the EU–US Privacy Shield. In the case of LotaData, the FTC also alleged that the company had falsely claimed certified

participation in the EU–US Privacy Shield framework. Lastly, the FTC had alleged that EmpiriStat Inc falsely claimed current participation in the EU–US Privacy Shield after its certification had lapsed, failed to verify annually that its statements related to its Privacy Shield practices were accurate, and failed to affirm it would continue to apply Privacy Shield protections to personal information it collected while participating in the framework. In each of these cases, as part of the settlements, each of the companies was prohibited from misrepresenting its participation in the Privacy Shield framework, as well as any other privacy or data security program sponsored by any government, or any self-regulatory or standard-setting organisation.

Invalidation of the Privacy Shield framework

On 16 July 2020, the CJEU issued a landmark judgment in a case brought by Max Schrems – the privacy activist credited with initiating the downfall of Safe Harbor – deemed *Schrems II*. *Schrems II* was originally heard by Ireland's High Court after Schrems brought a claim against Facebook, questioning whether the methods under which technology firms transfer EU citizens' data to the US afford EU citizens adequate protection from US surveillance. Specifically, Schrems alleged that the EU Standard Contractual Clauses do not ensure an adequate level of protection for EU data subjects, on the basis that US law does not explicitly limit interference with an individual's right to protection of their personal data in the same way as EU data protection law does. Following the complaint, Ireland's Data Protection Commission brought proceedings against Facebook in the Irish High Court. In June 2019, Ireland's High Court referred the case to the CJEU to determine the legality of the methods used for data transfers through a set of 11 questions referred for a preliminary ruling. The preliminary questions primarily addressed the validity of the standard contractual clauses, but also concerned the EU-US Privacy Shield framework.

In *Schrems II*, the CJEU ruled that the EU–US Privacy Shield was not a valid mechanism to lawfully transfer EU personal data to the US. In the decision, the CJEU held that:

> *. . . the limitations on the protection of personal data arising from [US domestic law] on the access and use [of the transferred data] by US public authorities [. . .] are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.*

Further, the CJEU found that the EU–US Privacy Shield framework does not grant EU individuals actionable rights before a body offering guarantees that are substantially equivalent to those required under EU law. On those grounds, the CJEU declared the EU–US Privacy Shield invalid.

In the aftermath of the *Schrems II* decision, organisations that previously relied on the Privacy Shield to lawfully transfer EU personal data to the US were required to identify alternative data transfer mechanisms, or applicable derogations pursuant to article 49 of the GDPR, to continue transfers of personal data to the US. On 24 July 2020, the EDPB published a set of FAQs on the CJEU's decision. These FAQs confirmed that there was no grace period for companies that relied on the EU–US Privacy Shield framework during which they could continue transferring to the US without assessing the legal basis relied on for those transfers. Transfers based on the EU–US Privacy Shield framework were now, according to the EDPB, illegal. Certain EU data protection authorities also issued statements and guidance in the aftermath of the *Schrems II* decision, taking various stances on the implication of the ruling. For example, the UK Information Commissioner's Office issued a statement that it stood 'ready to support UK organisations [. . .] to ensure that global data flows may continue and that people's personal data is protected', and subsequently advised organisations to follow the EDPB's FAQs on the use of standard contractual clauses as 'this guidance still applies to UK controllers and processors'. Certain German data protection authorities took stronger approaches, such as the Berlin data protection commissioner, who called on Berlin-based companies to recall EU data currently stored in the US back to the EU.

The US Department of Commerce also issued two new sets of FAQs following the Schrems II ruling. The new FAQs state that although (as a result of the ruling) the Privacy Shield:

> *. . . is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States . . . this decision does not relieve participants in the EU–US Privacy Shield of their obligations under the EU–US Privacy Shield Framework.*

The FAQs further state that the Department of Commerce will continue to administer the Privacy Shield program, including processing applications for self-certification and recertification and maintaining the list of Privacy Shield-certified organisations. The FAQs also make clear that organisations that wish to remain on the Privacy Shield list must continue to annually recertify to the Privacy Shield framework, including paying the annual processing fee. As of the date of this writing, the Department of Commerce has taken the view that continued participation in the Privacy Shield 'demonstrates a serious commitment to protect personal information in accordance with a set of privacy principles that offer meaningful privacy protections and recourse for EU individuals'.

Regarding the Swiss-US Privacy Shield, the CJEU decision did not strictly affect the legality of that framework, so the Swiss-US Privacy Shield remains a valid transfer mechanism. However, on 16 July 2020, the Federal Data Protection and Information Commissioner of Switzerland (FDPIC) issued a statement that the it 'has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDPIC will examine the judgement in detail and comment on it in due course'.

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@huntonak.com

Maeve Olney
molney@huntonak.com

200 Park Avenue
New York, NY 10166
United States
Tel: +1 212 309 1000
Fax: +1 212 309 1100

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772

www.huntonak.com

Belgium

David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The European Union's General Data Protection Regulation (GDPR) has become directly applicable in Belgium on 25 May 2018.

In the context of this important evolution of the legal framework, the Belgian data protection supervisory authority (formerly called the Commission for the Protection of Privacy) has been reformed by the Act of 3 December 2017 creating the Data Protection Authority (DPA). This reform was necessary to enable the DPA to fulfil the tasks and exercise the powers of a supervisory authority under the GDPR.

On 5 September 2018, the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Data Protection Act) was published in the Belgian Official Gazette. The Data Protection Act addresses the areas where the GDPR leaves room for EU member states to adopt country-specific rules and implements Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (the Directive). The Data Protection Act replaced the Act on the Protection of Privacy in relation to the Processing of Personal Data of 8 December 1992.

This chapter mainly focuses on the legislative data protection framework for private sector companies and does not address the specific regime for the processing of PII by police and criminal justice authorities in detail. The responses reflect the requirements set forth by the GDPR and the Data Protection Act.

In addition to the GDPR, a number of international instruments on privacy and data protection apply in Belgium, including:

the Council of Europe Convention 108 on the Protection of Privacy and Trans-border Flows of Personal Data;

- the European Convention on Human Rights and Fundamental Freedoms (article 8 on the right to respect for private and family life); and
- the Charter for Fundamental Rights of the European Union (article 7 on the right to respect for private and family life and article 8 on the right to the protection of personal data).

There is also sector-specific legislation relevant to the protection of PII. The Electronic Communications Act of 13 June 2005 (the Electronic Communications Act), for instance, imposes specific privacy and data protection obligations on electronic communications service providers.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Belgian Commission for the Protection of Privacy has been replaced by the Belgian DPA. The DPA is responsible for overseeing compliance with data protection law in Belgium. The DPA is headed by a chairperson and consists of five main departments, each headed by a director:

- a general secretariat that supports the operations of the DPA and has a number of executive tasks, including establishing the list of processing activities that require a data protection impact assessment, rendering opinions in case of prior consultation by a data controller, and approving codes of conduct and certification criteria, as well as standard contractual clauses and binding corporate rules for cross-border data transfers;
- a front office service that is responsible for receiving complaints and requests, starting mediation procedures, raising awareness around data protection with the general public and informing organisations of their data protection obligations;
- a knowledge centre that issues advice on questions related to PII processing and recommendations regarding social, economic or technological developments that may have an impact on PII processing;
- an investigation service that is responsible for investigating data protection law infringements; and
- a litigation chamber that deals with administrative proceedings.

Together, the chairperson and the four directors form the executive committee that, among others, approves the DPA's annual budget and determines the strategy and management plan. The Belgian DPA's 2020-2025 Strategic Plan was published on 12 March 2020.

In addition, there is an independent reflection board that provides non-binding advice to the DPA on all data-protection-related topics, upon request of the executive committee or the knowledge centre or on its own initiative.

To fulfil its role, the DPA has been granted a wide variety of investigative, control and enforcement powers. The enforcement powers include the power to:

- issue a warning or a reprimand;
- order compliance with an individual's requests;
- order to inform affected individuals of a security incident;
- order to freeze or limit processing;
- temporarily or permanently prohibit processing;
- order to bring processing activities in compliance with the law;
- order the rectification, restriction or deletion of PII and the notification thereof to data recipients;
- order the withdrawal of a licence given to a certification body;
- impose penalty payments and administration sanctions; and
- suspend data transfers.

Furthermore, the DPA can transmit a case to the public prosecutor for criminal investigation and prosecution. The DPA can also publish the decisions it issues on its website. The investigation powers of the DPA include the power to:

- hear witnesses;
- perform identity checks;
- conduct written inquiries;
- conduct on-site inspections;
- access computer systems and copy all data such systems contain;
- access information electronically;
- seize or seal goods, documents and computer systems; and
- request the identification of the subscriber or regular user of an electronic communication service or electronic communication means.

The investigation service also has the power to take interim measures, including suspending, limiting or freezing PII processing activities.

In addition to the DPA, certain public bodies, such as police agencies, intelligence and security services and the Coordination Unit for Threat Analysis, have a specific authority overseeing their data protection compliance.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The DPA is required to cooperate with all other Belgian public and private actors involved in the protection of individuals' rights and freedoms, particularly with respect to the free flow of PII and customer protection. The DPA must also cooperate with the national data protection authorities of other countries. Such cooperation will focus on, inter alia, the creation of centres of expertise, the exchange of information, mutual assistance for controlling measures and the sharing of human and financial resources. The rules for ensuring a consistent application of the GDPR throughout the EU set forth in the GDPR will apply in cross-border cases.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The DPA has the power to impose the administrative sanctions set forth in the GDPR. Depending on the nature of the violation, these administrative sanctions can go up to €20 million or 4 per cent of an organisation's total worldwide annual turnover of the preceding financial year. Breaches of data protection law can also lead to criminal penalties, which can, depending on the nature of the violation, go up to €240,000. In addition, violations of Belgian privacy and data protection law may result in civil action for damages.

SCOPE

Exempt sectors and institutions

5 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Belgian data protection law is generally intended to cover the processing of personally identifiable information (PII) by all types of organisations in all sectors. That being said, certain types of PII processing are (partially) exempted or subject to specific rules, including the processing of PII:

- by a natural person in the course of a purely personal or household activity; for example, a private address file or a personal electronic diary;
- solely for journalism purposes, or purposes of academic, artistic or literary expression;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- by the intelligence and security services;
- by the armed forces;
- by competent authorities in the context of security classification, clearances, certificates and advice;
- by the Coordination Unit for Threat Assessment;
- by the Passenger Information Unit; and
- by certain public bodies that monitor the police, intelligence and security services (such as the Standing Policy Monitoring Committee and the Standing Intelligence Agencies Review Committee).

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The General Data Protection Regulation (GDPR) and the Data Protection Act generally apply to the processing of PII in connection with the interception of communications and electronic marketing, as well as monitoring and surveillance of individuals. In addition, these topics are addressed by specific laws and regulations, including:

- the Belgian Criminal Code, the Electronic Communications Act and Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications (interception of communications);
- the Belgian Code of Economic Law, and the Royal Decree of 4 April 2003 regarding spam (electronic marketing); and
- the Belgian Act of 21 March 2007 on surveillance cameras (as amended by the Act of 21 March 2018), the Royal Decree of 10 February 2008 regarding the signalling of camera surveillance (as amended by the Royal Decree of 28 May 2018), the Royal Decree of 9 March 2014 appointing the categories of individuals authorised to watch real-time images of surveillance cameras in public spaces, and the Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace (surveillance of individuals).

Other laws

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

A significant number of laws and regulations set forth specific data protection rules that are applicable in a certain area, for example:

- the Act of 21 August 2008 on the establishment and organisation of the e-Health Platform (e-health records);
- Book VII of the Belgian Code of Economic Law on payment and credit services containing data protection rules for the processing of consumer credit data (credit information);
- Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications and the Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace;
- the Passenger Data Processing Act of 25 December 2016; and
- the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and the restriction on the use of cash.

PII formats

8 | What forms of PII are covered by the law?

The GDPR and the Data Protection Act apply to the processing of PII, wholly or partly by automatic means, and to the processing other than by automatic means of PII that forms part of a filing system (or is intended to form part of a filing system). PII is broadly defined and includes any information relating to an identified or identifiable natural person.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Belgian data protection law applies to processing of PII carried out in the context of the activities of an establishment of a controller or processor in Belgium. In addition, Belgian data protection law can also apply to the processing of PII by organisations that are established outside the European Union. This is the case where such organisations process PII of individuals located in Belgium in relation to offering goods or services to such individuals in Belgium or monitoring the behaviour of such individuals in Belgian territory.

Belgian data protection law will, however, not apply to the processing of PII by a processor established in Belgium on behalf of a controller established in another EU member state, to the extent that the processing takes place in the territory of the member state where the controller is located. In such a case, the data protection law of the member state where the controller is established will apply.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

In principle, all types of PII processing fall within the ambit of Belgian data protection law, regardless of who is 'controlling' the processing or merely processing PII on behalf of a controller. The 'controller' is any natural or legal person, public authority, agency or other body that alone or jointly with others determines the purposes and means of the processing of PII. Controllers can engage a 'processor' to carry out PII processing activities on their behalf and under their instructions. Controllers are subject to the full spectrum of data protection obligations. Processors, on the other hand, are subject to a more limited set of direct obligations under Belgian data protection law (including the obligation to process PII only on the controller's instructions, keep internal records of PII processing activities, cooperate with the data protection supervisory authorities, implement appropriate information security measures, notify data breaches to the controller, appoint a data protection officer if certain conditions are met and ensure compliance with international data transfer restrictions). In addition to these direct legal obligations, certain data protection obligations will be imposed on processors through their mandatory contract with the controller.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 | Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Controllers are required to have a legal basis for each personally identifiable information (PII) processing activity. The exhaustive list of potential legal grounds for processing of PII set forth in the General Data Protection Regulation (GDPR) will be available to controllers that are subject to Belgian data protection law:

- the data subject has unambiguously consented to the processing of his or her PII;
- the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation under EU or member state law to which the controller is subject;
- the processing is necessary in order to protect the vital interests of the data subject or another individual;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller; or
- the processing is necessary for the legitimate interests of the controller (or a third party to whom the PII is disclosed), provided that those interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

For certain types of PII, such as sensitive PII, more restrictive requirements in terms of legal bases apply. Furthermore, controllers that rely on consent to legitimise the processing of PII that takes place in the context of offering information society services to children below the age of 13 years must obtain consent from the child's legal representative.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

The processing of sensitive PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data, health data or data concerning a person's sex life or sexual orientation, is prohibited in principle, and can only be carried out if:

- the data subject has given his or her explicit consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller or the data subject in the employment, social security or social protection law area;
- the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent;
- the processing is carried out by a foundation, association or any other non-profit organisation with political, philosophical, religious or trade union objectives in the course of its legitimate activities, and solely relates to the member or former members of the organisation or to persons that have regular contact with the organisation and the PII is not disclosed to third parties without the data subjects' consent;
- the processing relates to PII that has been manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest recognised by EU or member state law;
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or member state law or pursuant to a contract with a health professional, subject to appropriate confidentiality obligations;
- the processing is necessary for reasons of public interest in the area of public health on the basis of EU or member state law; or

- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or member state law.

The Data Protection Act explicitly lists a number of PII processing activities that (provided certain conditions are met) can be deemed as necessary for reasons of substantial public interest, including PII processing activities of human rights organisations, the Centre for Missing and Sexually Exploited Children (Child Focus), and organisations that assist sex offenders.

The GDPR, prohibits the processing of PII relating to criminal convictions and offences or related security measures, except where the processing is carried out under the supervision of an official authority or when the processing is authorised by EU or member state law. The Data Protection Act allows the processing of PII relating to criminal convictions and offences:

- by natural persons, private or public legal persons for managing their own litigation;
- by lawyers or other legal advisors, to the extent that the processing is necessary for the protection of their clients' interests;
- by other persons, if the processing is necessary to perform duties of substantial public interest which are determined by EU or member state law;
- if the processing is required for scientific, historical or statistical research or archiving;
- if the data subject has given his or her explicit and written consent to the processing of PII relating to criminal convictions and offences for one or more purposes and the processing is limited to such purposes; or
- if the processing concerns PII made public by the data subject, on its own initiative, for one or more specific purposes and the processing is limited to such purposes.

The Data Protection Act also sets forth a number of specific measures that must be implemented when processing genetic, biometric, health data or PII relating to criminal convictions and offences. In such cases, a list of categories of individuals that will have access to the data, together with a description of those individuals' roles with respect to the processing, must be maintained. This list must be made available to the DPA upon request. Furthermore, the controller or processor must ensure that the individuals who have access to such data are bound by legal, statutory or contractual confidentiality obligations.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Controllers are required to provide notice to data subjects whose personally identifiable information (PII) they process. If PII is obtained directly from the data subject, the notice must contain at least the following information and be provided no later than the moment the PII is obtained:

- the name and address of the controller (and of its representative, if any);
- the contact details of the data protection officer (if any);
- the purposes of and legal basis for the processing;
- where the legitimate interests' ground is relied upon, the interests in question;
- the existence of the right to object, free of charge, to the intended PII processing for direct marketing purposes;
- the (categories of) recipients of PII;
- details of transfers to third countries or international organisations, the relevant safeguards associated with such transfers (including the existence or absence of an adequacy decision of the European Commission) and the means by which data subjects can obtain a copy of these safeguards or where they have been made available;
- the data retention period or criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of PII or the restriction of processing of PII or to object to the processing, as well as the right to data portability;
- the existence of the right to withdraw consent at any time if the controller relies on the data subject's consent for the processing of his or her PII;
- the right to lodge a complaint with a supervisory authority;
- whether providing the PII is a statutory or contractual requirement or a requirement to enter into a contract, as well as whether the data subject is obliged to provide the PII and the possible consequences of the failure to provide the PII; and
- information on automated individual decision-making (if any), including information on the logic involved in such decision-making, the significance and the envisaged consequences.

If PII is not obtained directly from the data subject, the controller must provide, in addition to the information listed above, the categories of PII concerned and the source from which the PII originates. This information must be provided within a reasonable period after obtaining the PII (within one month at the latest), or when PII is shared with a third party, at the very latest when the PII is first disclosed or when the PII is used to communicate with the data subject at the latest at the time of the first communication.

Exemption from notification

14 | When is notice not required?

Notice is not required if data subjects have already received the following information:

- the name and address of the controller (and of its representative, if any);
- the contact details of the data protection officer (if any);
- the purposes of and legal basis for the processing;
- where the legitimate interests' ground is relied upon, the interests in question;
- the existence of the right to object, free of charge, to the intended PII processing for direct marketing purposes;
- the (categories of) recipients of PII;
- details of transfers to third countries or international organisations, the relevant safeguards associated with such transfers (including the existence or absence of an adequacy decision of the European Commission) and the means by which data subjects can obtain a copy of these safeguards or where they have been made available;
- the data retention period or criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of PII or the restriction of processing of PII or to object to the processing, as well as the right to data portability;
- the existence of the right to withdraw consent at any time if the controller relies on the data subject's consent for the processing of his or her PII;
- the right to lodge a complaint with a supervisory authority;
- whether providing the PII is a statutory or contractual requirement or a requirement to enter into a contract, as well as whether the data subject is obliged to provide the PII and the possible consequences of the failure to provide the PII; and

- information on automated individual decision-making (if any), including information on the logic involved in such decision-making, the significance and the envisaged consequences.

In addition, in cases where PII is not collected directly from the data subject, the controller is exempt from the duty to provide notice if:

- informing the data subject proves impossible or would involve a disproportionate effort, in particular in the context of processing PII for archiving purposes in the public interest, statistical, historical or scientific research, or to the extent that providing notice would seriously impair or render the achievement of the purposes of the processing impossible; or
- PII must remain confidential subject to an obligation of professional secrecy regulated by EU or member state law.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Belgian data protection law includes a number of rights aimed at enabling data subjects to exercise choice and control over the use of their PII. In particular, data subjects are entitled to:

- request the controller to provide information regarding the processing of their PII and a copy of the PII being processed;
- obtain the rectification of incorrect PII relating to them and to have incomplete PII completed;
- obtain the erasure of their PII;
- obtain the restriction of the processing of their PII;
- receive the PII they have provided to the controller in a structured, commonly used and machine-readable format and to have it transmitted directly to another controller where technically feasible;
- object to the processing of their PII, for reasons related to their particular situation, if such processing is based on the ground that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or on the basis of the legitimate interests ground, unless the controller demonstrates that it has compelling legitimate grounds that outweigh the interests, rights and freedoms of the data subject or the processing is necessary for the establishment, exercise or defence of legal claims;
- object to the processing of their PII for direct marketing purposes; and
- not be subject to decisions having legal effects or similarly significantly affecting them, which are taken purely on the basis of automatic PII processing, including profiling.

The above-mentioned data protection rights are not absolute and typically subject to conditions and exemptions set forth in the GDPR and the Data Protection Act.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

Controllers must ensure that the PII they process is accurate and take reasonable steps to ensure that inaccurate PII is rectified or erased without delay.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

Controllers are required to limit the processing of PII to what is strictly necessary for the processing purposes. In terms of data retention requirements, PII must not be kept in an identifiable form for longer than necessary in light of the purposes for which the PII is collected or further processed. This means that, if a controller no longer has a need to identify data subjects for the purposes for which the PII was initially collected or further processed, the PII should be erased or anonymised.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Belgian data protection law incorporates the 'finality principle' and, therefore, PII can only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

PII can be processed for new purposes if these are not incompatible with the initial purposes for which the PII was collected, taking into account all relevant factors, especially the link between the purposes for which the PII was collected and the purposes of the intended further processing, the context in which the PII was collected, the relationship between the controller and the data subject, the nature of the concerned PII, the possible consequences of the further processing and the safeguards implemented by the controller (eg, pseudonymising or encrypting the PII). Furthermore, the Data Protection Act sets forth specific rules for the further processing of PII for archiving in the public interest, scientific or historical research or statistical purposes.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Controllers and processors are required to implement appropriate technical and organisational measures to protect personally identifiable information (PII) from accidental or unauthorised destruction, loss, alteration, disclosure, access and any other unauthorised processing.

These measures must ensure an appropriate level of security taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the varying likelihood and severity for the rights and freedoms of individuals.

These measures may include:

- the pseudonymisation and encryption of PII;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PII in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The more sensitive the PII and the higher the risks for the data subject, the more precautions have to be taken. The Data Protection Act, for instance, sets forth specific measures that controllers must implement when processing genetic and biometric data, health data and data relating to criminal convictions and offences, including measures to ensure that persons having access to such PII are under appropriate confidentiality obligations.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Electronic Communications Act imposes a duty on providers of publicly available electronic communications services to notify security breaches, under certain conditions, to the Data Protection Authority (DPA). The notification should contain the following information:

- the nature of the security breach;
- the consequences of the breach;
- details of the person or persons who can be contacted for more information concerning the breach;
- measures suggested or implemented by the controller to address the breach; and
- measures recommended to mitigate the negative effects of the security breach.

Where feasible, the notification should be done within 24 hours after detection of the breach. In case the controller does not have all required information available within this time-frame, it can complete the notification within 72 hours after the initial notification. The DPA has published a template form on its website to accommodate companies in complying with their data breach notification obligations. In addition, data subjects must be informed without undue delay when the security breach is likely to adversely affect their privacy or PII.

Since 25 May 2018, mandatory data breach notification obligations are no longer limited to the telecom sector. Controllers in all sectors are now required to notify data breaches to the DPA, unless the data breach is unlikely to result in a risk to the rights and freedoms of individuals. Such notification must be done without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Where notifying the DPA within 72 hours is not possible, the controller must justify such delay. A data breach notification to the DPA must at least contain:

- the nature of the data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of PII records concerned;
- the name and contact details of the data protection officer (if any) or another contact point to obtain additional information regarding the data breach;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken to address the breach, including mitigation measures where appropriate.

In addition to notifying the DPA, controllers are required to notify data breaches to the affected data subjects where the breach is likely to result in a high risk to the rights and freedoms of natural persons. The notification to the affected individuals must contain at least:

- the name and contact details of the data protection officer or another contact person;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken to address the breach, including mitigation measures where appropriate.

Notifying the affected individuals is, however, not required if the controller has implemented measures that render the affected PII unintelligible to any person who is not authorised to access it (eg, encryption), subsequent measures have been taken to ensure that the high risk to the rights and freedoms of individuals is no longer likely to materialise or where notifying the affected individuals would involve disproportionate effort. In the latter case, a public communication or similar measure should be made to inform the affected individuals about the breach. If a processor suffers a data breach, it must notify the controller on whose behalf it processes PII without undue delay. In Belgium, data breaches can be notified to the DPA via an online form made available on the DPA's website.

INTERNAL CONTROLS

Data protection officer

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a data protection officer is mandatory where:

- the processing is carried out by a public authority or body;
- the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or processor consist of processing sensitive personally identifiable information (PII) on a large scale.

In addition, the Data Protection Act provides that the appointment of a data protection officer is required for:

- private organisations that process PII on behalf of a public authority (as data processors) or that receive PII from a public authority and the processing of such PII is considered to present a high risk; and
- controllers processing PII for archiving purposes in the public interest or for scientific, historical or statistical purposes.

The main tasks of the data protection officer are to:

- inform and advise the controller or processor of its data protection obligations;
- monitor compliance with data protection laws, the General Data Protection Regulation (GDPR) and the controller's or processor's policies, including with respect to the assignment of responsibilities, raising awareness and training the controller's or processor's personnel involved in the processing of PII;
- assist with data protection impact assessments;
- cooperate with the relevant supervisory authority; and
- act as contact point for the data subjects and the relevant supervisory authorities regarding the processing activities, including prior consultation in the context of data protection impact assessments.

Although the obligation to maintain internal records of processing ultimately falls on the controller or processor, the data protection officer may also be assigned with the task of maintaining such records.

Controllers and processors must communicate the identity and contact details of their data protection officer to the Data Protection Authority (DPA) via an online form available on the DPA's website.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Controllers and processors are required to maintain internal records of their processing activities. Such records should be in writing, including in electronic form, and should be made available to the DPA upon request.

Controllers' internal records should contain, at least:

- the name and contact details of the controller, joint controller or the controller's representative, if applicable, and the identity and contact details of the data protection officer (if any);
- the purposes of the processing;
- a description of the categories of data subjects and PII;
- the categories of data recipients, including recipients in third countries;
- transfers of PII to a third country, including the identification of such country and, where applicable, documentation of the safeguards that have been put in place to protect the PII transferred;
- the envisaged data retention period or the criteria used to determine the retention period; and
- a description of the technical and organisational security measures put in place, where possible.

Processors' records should contain, at least:

- the name and contact details of the processor and each controller on behalf of which the processor is acting and, where applicable, the controller's or processor's representative and data protection officers;
- the categories of processing carried out on behalf of the controller;
- transfers of PII to third countries, including the identification of such countries and, where applicable, documentation of the safeguards put in place to protect the PII transferred; and
- where possible, a description of the technical and organisational security measures that have been put in place.

Companies that employ fewer than 250 persons are exempted from the obligation to keep internal records of their PII processing activities, unless their processing activities are likely to result in a risk to the rights and freedoms of individuals, are not occasional or include the processing of sensitive PII or PII relating to criminal convictions and offences.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The GDPR introduces the principles of privacy by design and privacy by default. Privacy by design means that controllers are required to implement appropriate technical and organisational measures designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR. When doing so, controllers must take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing. Privacy by default means that controllers must implement appropriate technical and organisational measures to ensure that, by default, only PII that is strictly necessary for each processing purpose is processed.

When engaging in new PII processing activities or changing existing processing activities that are likely to result in a high risk to the rights and freedoms of individuals, controllers are also required to carry out a data protection impact assessment. High-risk PII processing activities triggering the requirement to conduct a data protection impact assessment include:

- automated individual decision-making;
- large-scale processing of sensitive PII or PII relating to criminal convictions and offences; and
- systematic monitoring of a publicly accessible area on a large scale.

Where a data protection impact assessment reveals that the processing would result in a high risk and no measures are taken by the controller to mitigate such risk, the controller must consult the DPA prior to commencing the envisaged PII processing activity. The Data Protection Act excludes, under certain conditions, processing activities for journalistic, academic, artistic or literary purposes from such requirement.

The DPA has issued a Recommendation (01/2018) on data protection impact assessments in which it provides guidance to controllers on when a data protection impact assessment is required and what the assessment should contain. The Recommendation also includes a list of PII processing activities that require a data protection impact assessment and a list of PII processing activities that do not trigger the requirement to conduct a data protection impact assessment. In addition, the Belgian DPA issued a form that should be used in cases where prior consultation with the DPA is required. The form is available on the DPA's website.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

Since 25 May 2018, the obligation for controllers to register their data processing activities with the Data Protection Authority (DPA) no longer exists. Instead, controllers and processors are required to maintain internal records of their processing activities. However, if a controller or processor appoints a data protection officer, such appointment must be communicated to the DPA through a specific online form made available on the DPA's website.

Formalities

26 | What are the formalities for registration?

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Public access

29 | Is the register publicly available? How can it be accessed?

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Other transparency duties

31 | Are there any other public transparency duties?

No.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the General Data Protection Regulation (GDPR), when a controller outsources data processing activities to a third party (ie, a processor), it should put in place an agreement with the processor that sets out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of PII and categories of data subjects; and
- the obligations and rights of the controller.

Such agreement should stipulate that the processor:

- Processes the personally identifiable information (PII) only on documented instructions from the controller, unless otherwise required by EU or member state law. In that case, the processor must inform the controller of the legal requirement before processing, unless the law prohibits such information on important grounds of public interest. In addition, if in the processor's opinion an instruction of the controller infringes the GDPR, it should immediately inform the controller thereof.
- Ensures that persons authorised to process the PII have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Takes all appropriate technical and organisational measures required under the GDPR to protect the PII.
- Shall not engage sub-processors without the specific or general written authorisation of the controller. In the case of a general written authorisation, the processor must inform the controller of intended changes concerning the addition or replacement of sub-processors.
- Assists the controller by appropriate technical and organisational measures, insofar as this is possible, with data subjects' rights requests.
- Assists the controller in ensuring compliance with the security and data breach notification requirements, as well as the controller's obligation to conduct privacy impact assessments.
- At the end of the provision of the services to the controller, returns or deletes the PII, at the choice of the controller, and deletes existing copies unless further storage is required under EU or member state law.
- Makes available to the controller all information necessary to demonstrate compliance with the GDPR and contribute to audits.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

In general, there are no specific restrictions under the GDPR or the Data Protection Act on the disclosure of PII other than the restrictions resulting from the general data protection principles (such as lawfulness, notice and purpose limitation).

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

PII can be transferred freely to other countries within the European Economic Area (EEA), as well as to countries recognised by the European Commission as providing an 'adequate level of data protection'. A list of countries deemed to be providing an adequate level of data protection is available on the European Commission's website.

Transferring PII to countries outside the EEA that are not recognised as providing an 'adequate level of data protection' is prohibited unless:

- the data subject has explicitly given his or her consent to the proposed transfer after having been informed of the possible risks of such transfers;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;
- the transfer is necessary for important reasons of public interest, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or other persons;
- the transfer is made from a register that is open to consultation either by the public in general or by any person that can demonstrate a legitimate interest; or
- if none of the above applies and no appropriate safeguards have been put in place, the transfer can take place if it is necessary for the purposes of compelling legitimate interests pursued by the controller, but only if the transfer is not repetitive, concerns only a limited number of data subjects, and the controller has assessed all circumstances surrounding the data transfer and has provided suitable safeguards to protect the PII. In this case, the controller must inform the DPA and concerned data subjects of the transfer and the legitimate interests that justify such transfer.

In addition to the exemptions listed above (which should typically only be relied on in limited cases), cross-border transfers to non-adequate countries are allowed if the controller has implemented measures to ensure that the PII receives an adequate level of data protection and data subjects are able to exercise their rights after the PII has been transferred. Such measures include the execution of standard contractual clauses approved by the European Commission or adopted by a supervisory authority, an approved code of conduct or certification mechanism or implementation of binding corporate rules. In addition, transfers of PII can be legitimised by executing an ad hoc data transfer agreement. However, in such cases the prior authorisation of the DPA must be obtained.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

In general, cross-border data transfers do not need to be notified to the DPA.

Prior authorisation is required if the controller relies on an ad hoc data transfer agreement to legitimise the transfer of PII to non-adequate countries. Such authorisation is not required when the controller has guaranteed an adequate level of data protection by executing the standard contractual clauses approved by the European Commission.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The data transfer restrictions and authorisation requirements apply regardless of whether PII is transferred to a service provider (ie, processor) or another controller.

The restrictions and requirements applicable to onward PII transfers depend on the legal regime in the jurisdiction where the data importer is located and the data transfer mechanism relied upon to legitimise the initial data transfer outside the EEA. For example, the standard contractual clauses contain specific requirements for onward data transfers.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Data subjects have a right to 'access' the personally identifiable information (PII) that a controller holds about them. When a data subject exercises his or her right of access, the controller is required to provide the following information to the data subject:

- confirmation as to whether the controller processes the data subject's PII;
- the purposes for which his or her PII is processed;
- the categories of PII concerned;
- the recipients or categories of recipients to whom PII has been or will be disclosed, in particular, recipients in third countries, and in case of transfers to third countries, the appropriate safeguards put into place by the controller to legitimise such transfers;
- where possible, the envisaged period for which the PII will be stored or, if not possible, the criteria used to determine such period;
- the existence of the right to request the rectification or erasure of PII or restriction of the processing or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- information regarding the source of the PII; and
- the existence of automated decision-making and information about the logic involved in any such automated decision-making (if any), as well as the significance and the envisaged consequences of such processing.

The controller should also provide a copy of the PII to the data subject in an intelligible form. For further copies requested by the data subjects, controllers may charge a reasonable fee to cover administrative costs.

The right to obtain a copy of PII may be subject to restrictions to the extent it adversely affects the rights and freedoms of others, and the controller may refuse to act on a request of access if the request is manifestly unfounded or excessive, in particular because of its repetitive character.

In addition, exemptions to the right of access apply to PII originating from certain public authorities, including the police and intelligence services and to PII processed for journalistic, academic, artistic or literary purposes.

Other rights

38 | Do individuals have other substantive rights?

In addition to the right of access described above, data subjects have the following rights:

Rectification

Data subjects are entitled to obtain, without undue delay, the rectification of inaccurate PII relating to them.

Erasure ('right to be forgotten')

Data subjects have the right to request the erasure of PII concerning them where:

- the PII is no longer necessary for the purposes for which it was collected or otherwise processed;
- the processing is based on consent and the data subject withdraws his or her consent and there is no other legal basis for the processing;
- the data subject objects to the processing of his or her PII based on the controller's legitimate interests and there are no overriding legitimate grounds for the processing;
- the data subject objects to the processing of his or her PII for direct marketing purposes;
- PII has been unlawfully processed;
- PII has to be erased for compliance with a legal obligation under EU or member state law; and
- PII has been collected in relation to offering information society services to a child.

The right to be forgotten does not apply where the processing is necessary for:

- the exercise of the right to freedom of expression and information,
- compliance with a legal obligation under EU or member state law;
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- reasons of public interest in the area of public health;
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- the establishment, exercise or defence of legal claims.

Restriction of processing

Data subjects are entitled to request that the processing of their PII is restricted by the controller, where one of the following conditions applies:

- the data subject is contesting the accuracy of his or her PII, in which case, the processing should be restricted for a period enabling the verification by the controller of the accuracy of the PII;
- the processing is unlawful and the data subject opposes the erasure of the PII and requests the restriction of its use instead;
- the controller no longer needs the PII, but the PII is required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to the processing of his or her PII for purposes other than direct marketing, based on grounds relating to his or her particular situation. In this case, the processing should be restricted, pending the verification by the controller as to whether the controller's legitimate interests override those of the data subject.

Objection to processing

Data subjects have the right to object at any time to the processing of their PII for substantial and legitimate reasons related to their particular situation, where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or where the controller processes the PII to pursue its legitimate interests. In addition, data subjects are in any event (ie, without any specific justification) entitled to object, at any time, to the processing of their PII for direct marketing purposes.

Data portability

Data subjects are entitled to receive in a structured, commonly used and machine-readable format the PII they have provided directly to the controller and the PII they have provided indirectly by virtue of the use of the controller's services, websites or applications. In addition, where technically feasible, data subjects have the right to have their PII transmitted by the controller to another controller. The right to data portability only applies if:

- the PII is processed on the basis of the data subject's consent or the necessity of the processing for the performance of a contract; and
- the PII is processed by automated means.

The above-mentioned rights are subject to certain restrictions, in particular in the case of processing PII originating from certain public authorities, including the police and intelligence services, or processing of PII for journalistic, academic, artistic or literary purposes.

Complaint to relevant supervisory authorities and enforce rights in court

Data subjects are entitled to file a complaint with the Data Protection Authority (DPA) (which has been granted with investigative, control and enforcement powers) to enforce their rights. Furthermore, data subjects can initiate proceedings before the President of the Court of First Instance when their rights have not been respected by the controller.

Automated decision-making

Data subjects also have the right not to be subject to decisions having legal effects or significantly affecting them, including profiling, which are taken purely on the basis of automatic data processing, unless the decision:

- is necessary to enter into or for the performance of a contract;
- is based on a legal provision under EU or member state law; or
- is based on the data subject's explicit consent.

Compensation

39 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Data subjects are entitled to receive compensation from controllers if they have suffered material or non-material damages as a result of a violation of Belgian data protection law. Controllers will only be exempt from liability if they are able to prove that they are not responsible for the event giving rise to the damage. Individuals may choose to mandate an organ, organisation or a non-profit organisation to lodge a complaint on their behalf before the DPA or the competent judicial body.

Enforcement

40 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Enforcement of data subjects' rights is possible through legal action before the Belgian courts (ie, before the President of the Court of First Instance) and via the DPA.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No.

SUPERVISION

Judicial review

42 Can PII owners appeal against orders of the supervisory authority to the courts?

Controllers can appeal against certain decisions of the inspection service of the Data Protection Authority (DPA) (including orders to freeze or limit processing activities, decisions to temporarily or permanently prohibit the processing or decisions to seize or seal goods or computer systems) in front of the DPA's Litigation Chamber. In addition, controllers can appeal the decisions of the DPA's Litigation Chamber in front of a specific section of the Appeal Court of Brussels (ie, *Cour des Marchés or Marktenhof*).

SPECIFIC DATA PROCESSING

Internet use

43 Describe any rules on the use of 'cookies' or equivalent technology.

Cookies or any other type of information can only be stored or accessed on individuals' equipment provided that the individuals have consented after having been informed about the use of such cookies. However, individuals' opt-in consent is not required if the access to or storage of information on their equipment is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or is strictly necessary to provide a service explicitly requested by the individual.

On 9 April 2020, the Data Protection Authority (DPA) updated its practical guidance on cookies with a view to clarify how companies should inform individuals about and obtain their consent for the use of cookies, as well as the types of cookies that are exempted from the consent requirement.

The guidance provides that consent must be informed, unambiguous and provided through a clear affirmative action. Merely continuing to browse a website does not constitute valid consent. Users must have the possibility to provide granular consent per type of cookie, as well as, in a second stage, per cookie. In addition, users must be provided with information regarding the use of cookies. The DPA suggests providing this information in two phases: first, a notice at the time the users' consent is obtained, and second, a more detailed notice in the form of a cookie policy.

According to the DPA, users must be provided with the following information upon consenting to the use of cookies:

- the entity responsible for the use of cookies;
- the purposes for which cookies are used;
- the data collected through the use of cookies;
- the cookies' expiration time; and
- the users' rights with respect to cookies, including the right to withdraw their consent.

The DPA also clarifies that the lifespan of a cookie must be limited to what is necessary to achieve the cookie's purpose and cookies should not have an unlimited lifespan.

The cookie requirements under Belgian law result from the legal regime for the use of cookies set forth by the ePrivacy Directive 2002/58/EC (the ePrivacy Directive, as transposed into member state law). The ePrivacy Directive is currently under review and will most likely be replaced by the ePrivacy Regulation in the future. The exact timing of the adoption of the ePrivacy Regulation has, however, not yet been determined.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Apart from the general rules on marketing practices and specific rules on marketing for certain products or services (eg, medicines and financial services), there are specific rules for marketing by email, fax and telephone.

Marketing by electronic post

Sending marketing messages by electronic post (eg, email or SMS) is only allowed with the prior, specific, free and informed consent of the addressee. However, provided that certain conditions are fulfilled, electronic marketing to legal persons and existing customers is exempt from the opt-in consent requirement. In any event, electronic marketing messages should inform the addressee about his or her right to opt out from receiving future electronic marketing and provide appropriate means to exercise this right electronically. In addition to the consent requirement, Belgian law sets out specific requirements concerning the content of electronic marketing messages, such as the requirement that electronic marketing should be easily recognisable as such and should clearly identify the person on whose behalf it is sent.

Marketing by automated calling systems and fax

Direct marketing by automated calling systems (without human intervention) and fax also requires the addressees' prior, specific, free and informed consent. Furthermore, the addressee should be able to withdraw his or her consent at any time, free of charge and without any justification.

Marketing by telephone

Belgian law explicitly prohibits direct marketing by telephone to individuals who have registered their telephone number with the Do Not Call register.

As the rules on electronic communications marketing under Belgian law result from the ePrivacy Directive, these rules may change once the ePrivacy Directive is replaced by the ePrivacy Regulation (which has not been adopted yet). In addition, on 10 February 2020, the DPA published its Recommendation 1/2020 on data processing activities for direct marketing purposes, which aims at clarifying the complex rules relating to the processing of PII for direct marketing purposes and provides practical examples and guidelines around direct marketing.

Amongst others, Recommendation 1/2020 clarifies that:

- Determining and specifying the purposes for which PII will be processed is essential. In this respect, the DPA considers that merely stating that personal data will be processed for direct marketing purposes is not sufficient in light of the transparency requirements applicable under the GDPR.
- To ensure data minimisation, companies should limit open fields in data collection forms, review their databases on a regular basis to delete any unnecessary data, and implement processes to ensure that Do Not Call lists are taken into account when reviewing databases where marketing data is stored.
- Individuals must be offered a right to object at any time and easily, without having to take additional steps and free of charge, to the processing of their PII for direct marketing purposes. In this respect, the DPA considers that a simple 'unsubscribe' button in small characters at the end of a marketing email is not sufficient. In addition, where it is technically feasible, the DPA recommends allowing individuals to granularly select the marketing activities for which they want to object (eg, email marketing or SMS).
- Consent to direct marketing must be specific with respect to the content of the marketing communication and the means used.
- Where an individual withdraws their consent to the processing of PII, there is no longer a valid legal ground unless PII must be kept to comply with a legal obligation. In practice, this means that if the individual withdraws their consent and there is no alternative legal ground, PII should be deleted (regardless of whether the individual exercises their deletion rights). The same applies where individuals object to the processing of their PII on the basis of the legitimate interest ground.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules on the use of cloud computing services under Belgian law. However, the DPA has issued advice (Advice No. 10/2016 of 24 February 2016 on the Use of Cloud Computing by Data Controllers) that identifies the privacy risks related to cloud computing services and provides guidelines for data controllers on how to comply with Belgian data protection law when relying on providers of cloud computing services.

Some of the risks identified by the DPA include:

- loss of control over the data owing to physical fragmentation;
- increased risk of access by foreign authorities;
- vendor lock-in;
- inadequate management of access rights;
- risks associated with the use of sub-processors;
- non-compliance with data retention restrictions;
- difficulties with accommodating data subjects' rights;
- unavailability of the services;
- difficulties with recovering data in the case of termination of the cloud provider's business or the service contract; and
- violations of data transfer restrictions.

To address these risks, the DPA has issued a number of guidelines for data controllers that want to migrate data to a cloud environment. The DPA recommends data controllers, among others, to:

- clearly identify data and data processing activities before migrating them to the cloud environment, taking into account the nature and sensitivity of the data;
- impose appropriate contractual and technical requirements on cloud providers (eg, not allowing cloud providers to alter terms and conditions unilaterally, requiring cloud providers to inform about the use of sub-processors and including exhaustive lists of physical locations where data can be stored);
- identify the most suitable cloud solution;
- perform a risk analysis (ideally by an independent body specialised in information security);
- select the appropriate cloud provider, taking into account the risk analysis;
- inform data subjects about the migration of their PII to the cloud; and
- monitor changes to cloud services over time and update the risk analysis in light of such changes.

UPDATE AND TRENDS

Key developments of the past year

46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

On 12 March 2020, the Data Protection Authority (DPA) published its final 2020-2025 Strategic Plan, describing its vision for the years to come, defining the DPA's priorities and strategic objectives, as well as listing the means necessary to achieve those objectives. In the Strategic Plan, the DPA indicated that it will focus its actions for the coming five years on a number of sectors, including telecom and media, public authorities, direct marketing, education and small and medium-enterprises.

In addition, the DPA identified several aspects of the General Data Protection Regulation (GDPR) and topics it will be focusing on, including:

- the role of the data protection officer;
- lawfulness of data processing activities, and more particularly the processing of personally identifiable information (PII) based on the legitimate interests' legal basis;
- data subjects' rights;
- pictures and cameras;
- online processing of PII, including the use of cookies; and
- sensitive PII processing.

The DPA has also recently published various materials regarding the processing of PII in the context of the covid-19 pandemic, including a statement regarding health-related apps and PII processing at the work-place. The covid-19 related content is available on the DPA's website.

HUNTON ANDREWS KURTH

David Dumont
ddumont@huntonak.com

Laura Léonard
lleonard@huntonak.com

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
Tel: +32 2 643 58 00
Fax: +32 2 643 58 22
www.huntonak.com

United Kingdom

Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The primary legal instruments include the UK's Data Protection Act 2018 (DPA) and the EU's General Data Protection Regulation 2016/679 on the protection of individuals with regard to the processing of PII and the free movement of data (GDPR). The UK is a signatory to Treaty 108 of the Council of Europe. The UK has no national constitutional privacy provisions, but is bound by the EU Charter of Fundamental Rights.

In the 2016 referendum, the UK voted to leave the EU. In March 2017, the UK's government formally notified the EU of the UK's referendum decision, triggering article 50 of the EU's Lisbon Treaty. This signalled the beginning of the process of leaving the EU. The UK left the EU on 31 January 2020 and entered a Brexit transition period that will last until 31 December 2020. During the transition period, EU laws, including the GDPR, continue to apply in the UK and the Information Commissioner's Office (ICO) will continue to act as the lead supervisory authority for businesses and organisations operating in the UK. The UK has until 31 December 2020 to negotiate its future relationship with the EU, although this deadline may be extended.

Following the end of the transition period, the GDPR will no longer apply directly in the UK. However, UK organisations must still comply with its requirements after this point as the DPA enacted the GDPR's requirements in UK law. The UK government has issued a statutory instrument, the Data Protection, Privacy and Electronic Communications (Amendments, etc) Regulations 2019 (EU Exit), which amends the DPA and merges it with the requirements of the EU GDPR to form a data protection regime that will work in a UK context after Brexit. This new regime will be known as 'the UK GDPR'.

While the UK has left the EU, it remains unclear what future trading arrangements will be agreed between the UK and the EU following the end of the transition period. The UK has confirmed that it will seek adequacy status to enable data flows between the UK and the European Economic Area. This will require data protection laws that are essentially equivalent to EU data protection laws (ie, the GDPR) but may be complicated by the UK's Investigatory Powers Act 2016, which permits the type of bulk surveillance practices that the Court of Justice of the European Union believes fail to respect data protection principles. Further, non-EU controllers or processors that process the PII of EU data subjects in the context of offering goods or services to them or monitoring their behaviour will be subject to the GDPR in any event.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The DPA and the GDPR are supervised by the ICO. The ICO may:

- seek entry to premises subject to a warrant issued by a court;
- require the provision of information by service of information notices;
- by notice, require government departments to undergo a mandatory audit (referred to as 'assessment'); and
- conduct audits of private sector organisations with the consent of the organisation.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The ICO participates in the 'one-stop shop' under the GDPR, under which organisations with a main establishment in the EU may primarily be regulated by the supervisory authority of the jurisdiction in which the main establishment is located (lead supervisory authority). The DPA and the GDPR confer on the ICO powers to participate in the GDPR's one-stop shop, to cooperate with other concerned supervisory authorities, to request from and provide mutual assistance to other concerned supervisory authorities, and to conduct joint operations, including joint investigations and joint enforcement actions with other concerned supervisory authorities.

The status of the ICO's participation in the EU's one-stop shop once the UK has left the EU is currently not clear, but in the absence of an agreement stating otherwise, from 1 January 2021 the ICO will no longer be permitted to participate in the GDPR's one-stop shop mechanism. This eventuality would impact UK-based data controllers or data processors that are currently carrying out cross-border processing of PII, across EU member state borders.

The DPA also requires the ICO, in relation to third countries and international organisations, to take steps to develop cooperation mechanisms to facilitate the effective enforcement of legislation relating to the protection of personal data, to provide international mutual assistance in the enforcement of legislation for the protection of personal data, to engage relevant stakeholders in discussion and activities, and to promote the exchange and documentation of legislation and practice for the protection of personal data.

Breaches of data protection

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The ICO has a number of enforcement powers. Where a data controller or a data processor breaches data protection law, the ICO may:

- issue undertakings committing an organisation to a particular course of action to improve its compliance with data protection requirements;
- serve 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; and
- issue fines of up to the greater of €20 million or 4 per cent of annual worldwide turnover, depending on the nature of the violation of the DPA and GDPR.

A number of breaches may lead to criminal penalties. The following may constitute criminal offences:

- making a false statement in relation to an information notice validly served by the ICO;
- destroying, concealing, blocking or falsifying information with the intention of preventing the ICO from viewing or being provided with the information;
- unlawfully obtaining PII;
- knowingly or recklessly re-identifying PII that is de-identified without the consent of the data controller responsible for that PII;
- altering PII so as to prevent disclosure of the information in response to a data subject rights request;
- requiring an individual to make a subject access request; and
- obstructing execution of a warrant of entry, failing to cooperate or providing false information.

Criminal offences can be prosecuted by the ICO or by or with the consent of the Director of Public Prosecutions.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Exemptions from the full rigour of the law apply in some circumstances and for some instances of processing. A wide exemption applies to processing by individuals for personal and domestic use, but no sectors or institutions are outside the scope of the law. Recent European case law has clarified that this exemption applies only to 'purely domestic' or household activities, with no connection to a professional or commercial activity. This means that if personally identifiable information (PII) is only used for such things as writing to friends and family or taking pictures for personal enjoyment, such use of PII will not be subject to the General Data Protection Regulation (GDPR).

The GDPR and the Data Protection Act 2018 (DPA) apply to private and public sector bodies. That said, the processing of PII by competent authorities for law enforcement purposes is outside the scope of the GDPR (eg, the police investigating a crime). Instead, this type of processing is subject to the rules in part 3 of the DPA. In addition, PII processed for the purposes of safeguarding national security or defence is also outside the scope of the GDPR. However, it is covered by part 2, chapter 3 of the DPA (also known as the 'applied GDPR'), which contains an exemption for national security and defence.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended), although the GDPR and the DPA often apply to the same activities, to the extent that they involve the processing of PII. Interception and state surveillance are covered by the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. The interception of business communications is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

The law includes many provisions dealing with information; for example, the regulation of credit files is covered in the Consumer Credit Act 1974. Laws on e-commerce include provisions linked to the regulation of PII. Laws on defamation, copyright and computer misuse also affect data protection. However, there is no specific data protection sectoral legislation. The UK has a range of 'soft law' instruments, such as codes of practice for medical confidentiality or the management of information held for policing, that apply in specific sectoral areas.

The DPA requires the ICO to draw up and publish codes of practice that relate to data sharing, direct marketing, age-appropriate design and data protection, and journalism, and the ICO has published draft codes of practice on these issues. These draft codes are not yet in force and are either in the consultation phase. The ICO's Age Appropriate Design Code has received parliamentary approval and is due to come into force in autumn 2021.

While not specifically related to the protection of PII, the Network and Information Systems Regulations 2018 (NIS Regulations) are intended to establish a common level of security for network and information systems. The NIS Regulations aim to address, amongst other things, the threats posed by cyber-attacks.

PII formats

8 | What forms of PII are covered by the law?

The GDPR and the DPA cover PII held in electronic form plus such information held in structured files, called 'relevant filing systems'. In order to fall within this definition, the file must be structured by reference to individuals or criteria relating to them, so that specific information about a particular individual is readily accessible.

Ultimately, whether a manual file is part of a relevant filing system is a matter of fact as well as law, and must be considered on a case-by-case basis.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Organisations that are data controllers or data processors fall within the scope of the law if they are established in the UK and process PII in the context of that establishment, or if they are not established in the EU but offer goods or services to individuals located in the UK, or monitor the behaviour of individuals located in the UK.

A data controller or data processor is 'established' in the UK if it is resident in the UK, is incorporated or formed under the laws of

England and Wales, Scotland or Northern Ireland, or maintains and carries on activities through an office, branch, agency or other stable arrangements in the UK. Where a data controller or data processor is established in the UK, the DPA will apply regardless of whether the processing takes place in the UK or not.

Data controllers established outside the EU that are subject to the GDPR and the DPA must nominate a representative in the UK.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR and the DPA are applicable to data controllers (ie, those that decide the purposes and the means of the data processing) and data processors (who merely process PII on behalf of data controllers). As such, the data controllers are the main decision-makers and they exercise overall control over the purposes and means of the processing of PII. Data processors act on behalf of, and only on the instructions of, the relevant data controller.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The General Data Protection Regulation (GDPR) requires data controllers rely on a legal ground set forth in the GDPR for all processing of personally identifiable information (PII). Additional conditions must also be satisfied when processing sensitive PII.

The grounds for processing non-sensitive PII are:

- consent of the individual;
- performance of a contract to which the individual is party or in order to take steps at the request of the data subject prior to entering into a contract;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-European Union jurisdiction is not sufficient for the purposes of this ground);
- protection of the vital interests of the individual (ie, a life or death situation);
- the processing is necessary for carrying out public functions; or
- the processing is necessary for the legitimate interests of the data controller (or third parties to whom the PII is disclosed), unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

Distinct grounds for legitimate processing apply to the processing of sensitive PII (also known as 'special categories of PII'). 'Sensitive PII' is defined as PII relating to a data subject's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health;
- sex life or sexual orientation;
- genetic data;
- biometric data (when processed for the purpose of uniquely identifying a natural person);
- commissioning or alleged commissioning of any offence; or
- any proceedings for committed or alleged offences, the disposal of such proceedings of sentence of any court.

Where a controller processes sensitive PII it must establish both a ground for processing both non-sensitive PII (eg, consent, performance of a contract, etc) and a separate ground for processing sensitive PII. The GDPR sets forth a number of grounds that may be relied upon for the processing of sensitive PII, including:

- explicit consent of the individual;
- performance of employment law obligations;
- protection of the vital interests of the individual (ie, a life or death situation);
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, and the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the PII is not disclosed outside that body without the consent of the data subjects;
- the processing relates to PII, which is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or in order to exercise legal rights;
- processing for medical purposes;
- processing necessary for reasons of public interest in certain specific areas; or
- processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

In addition to the grounds set forth in the GDPR, the Data Protection Act 2018 (DPA) sets forth a number of additional grounds that also may be relied upon, including:

- processing necessary for monitoring and ensuring equality of opportunity or treatment;
- preventing or detecting unlawful acts;
- preventing fraud;
- processing to comply with regulatory requirements relating to establishing whether a person has committed unlawful acts or has been involved in dishonesty, malpractice or other seriously improper conduct; and
- in connection with administering claims under insurance contracts or exercising rights and complying with obligations arising in connection with insurance contracts.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Data controllers are obliged to notify individuals of:

- the data controller's identity and contact information and, where applicable, the identity and contact information of its representative;
- the contact details of the data controller's data protection officer (DPO), if it has appointed one;
- the purposes for which the personally identifiable information (PII) will be processed and the legal basis for processing;

- the legitimate interests pursued by the data controller, if applicable;
- the recipients or categories of recipients of the PII;
- the fact that the data controller intends to transfer the PII to a third country and the existence or absence of an adequacy decision by the European Commission, and a description of any safeguards (eg, EU Model Clauses) relied upon and the means by which individuals may obtain a copy of them;
- the period for which PII will be stored or the criteria used to determine that period;
- a description of the rights available to individuals;
- the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with an European Union data protection supervisory authority;
- whether the provision of PII is a statutory or contractual requirement, or is necessary to enter into a contract, as well as whether the individual is obliged to provide the PII and of the consequences of failure to provide such PII; and
- the existence of automated decision-making and, if so, meaningful information about the logic involved as well as the significance and envisaged consequences of the processing for the individual.

When PII is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the PII originated and the categories of PII obtained.

Notice must be provided at the time the PII is collected from the data subject. When PII is obtained from a source other than the data subject it relates to, the data controller needs to provide the data subject with the notice:

- within a reasonable period of obtaining the PII and no later than one month;
- if the data controller uses the data to communicate with the data subject, at the latest, when the first communication takes place; or
- if the data controller envisages disclosure to someone else, at the latest, when the data controller discloses the data.

Exemption from notification

14 | When is notice not required?

Where PII is obtained from a source other than the data subject, then provision of notice is not required if:

- the individual already has the information;
- the provision of such information would be impossible or require disproportionate effort (in which case the data controller shall take appropriate measures to protect data subjects, including making the relevant information publicly available);
- the provision of the information would render impossible or seriously impair the achievement of the objectives of the processing;
- obtaining or disclosure of the PII is required by EU law to which the data controller is subject; or
- where the PII is subject to an obligation of professional secrecy under UK or EU law.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals have a number of rights in relation to PII held by data controllers:

- to obtain confirmation of whether the data controller processes PII about the individual and to obtain a copy of that PII (also known as 'the right of access');
- to rectify PII that is inaccurate;
- to have PII erased in certain circumstances (eg, when the PII is no longer necessary for the purposes for which it was collected by the data controller);
- to restrict the processing of PII;
- to obtain a copy of PII in a structured, commonly used and machine-readable format, and to transmit that PII to a third-party data controller without hindrance, to the extent that it is technically feasible (also known as 'the right to data portability');
- to object to the processing of PII in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PII, except in particular circumstances.

Data processors are not required to comply with data subject rights requests, but are required to provide assistance to data controllers on whose behalf they process PII to respond to any such requests.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

The data controller must ensure that PII is relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

The data controller must ensure that PII is adequate, relevant and not excessive in relation to the purpose for which it is held. This means that the data controller should not collect or process unnecessary or irrelevant PII. The Data Protection Act 2018 and the General Data Protection Regulation do not impose any specified retention periods. PII may be held only for as long as is necessary for the purposes for which it is processed.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII may only be used for specified and lawful purposes, and may not be processed in any manner incompatible with those purposes. The purposes must be specified in the notice given to the individual.

In addition, recent case law has confirmed the existence of a tort of 'misuse of private information'. Under this doctrine, the use of private information about an individual for purposes to which the individual has not consented may give rise to a separate action in tort against the data controller, independent of any action taken under the DPA.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

PII may not be processed for new purposes unless the further purposes are lawful (ie, based on a lawful ground). It may be processed for a new purpose as long as that purpose is not incompatible with the original purpose, but notice of the new purpose must be provided to the individual. Where a new purpose would be incompatible with the original purpose, it must be legitimised by the consent of the individual unless an exemption applies. For example, PII may be further processed for certain specified public interest purposes, including the prevention of crime or prosecution of offenders and processing for research, historical or statistical purposes.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) do not specify the types of security measures that data controllers and data processors must take in relation to personally identifiable information (PII). Instead, data controllers and data processors must have in place 'appropriate technical and organisational measures' to protect against 'unauthorised or unlawful processing of [PII] and against accidental loss or destruction of, or damage to, [PII]'. In addition, the GDPR provides several examples of security measures that data controllers and data processors should consider implementing, including:

- the pseudonymisation and encryption of PII;
- the ability to restore the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to PII in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of the measures implemented.

Under the relevant provisions, in assessing what is 'appropriate' in each case, data controllers and processors should consider the nature of the PII in question and the harm that might result from its improper use, or from its accidental loss or destruction. The data controller and processor must take reasonable steps to ensure the reliability of its employees.

Where a data controller uses an outsourced provider of services to process PII, it must choose a data processor providing sufficient guarantees of security, take reasonable steps to ensure that these are delivered, require the data processor to enter into a contract in writing under which the data processor will, among other things, act only on the instructions of the controller and apply equivalent security safeguards to those imposed on the data controller.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The GDPR requires data controllers to notify the Information Commissioner's Office (ICO) of a data breach within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, data controllers must notify affected individuals of a breach without undue delay if the breach is likely to result in a high risk to the rights and freedoms of affected individuals. Data processors are not required to notify data breaches to supervisory authorities or to affected individuals, but must notify the relevant data controller of a data breach without undue delay.

In addition to notifying breaches to the ICO and to affected individuals, data controllers must also document all data breaches and retain information relating to the facts of the breach, its effects and the remedial action taken.

INTERNAL CONTROLS

Data protection officer

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The General Data Protection Regulation (GDPR) requires data controllers and data processors to appoint a data protection officer (DPO) if:

- the core activities of the data controller or data processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or processor consist of processing sensitive PII or PII relating to criminal offences and convictions on a large scale.

If appointed, a DPO is responsible for:

- informing and advising the data controller or data processor and its employees of his or her obligations pursuant to data protection law;
- monitoring compliance with the GDPR, awareness raising, staff training and audits;
- providing advice with regard to data protection impact assessments;
- cooperating with the Information Commissioner's Office (ICO) and other European Union data protection supervisory authorities; and
- acting as a contact point for the ICO on issues relating to processing PII.

Organisations may also elect to appoint a DPO voluntarily, although such an appointment will need to comply with the requirements of the GDPR.

Record keeping

23 Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Under article 30 of the GDPR, data controllers and data processors are required to retain internal records that describe the processing of PII that is carried out. These records must be maintained and provided to the ICO upon request.

For data controllers, the record must include the following information:

- the name and contact details of the data controller and, where applicable, the joint controller, and of the data controller's representative and DPO;
- the purposes of the processing;
- the data subjects and categories of PII processed;
- the categories of recipients to whom PII has been or will be disclosed;
- a description of any transfers of PII to third countries and the safeguards relied upon;
- the envisaged time limits for erasure of the PII; and
- a general description of the technical and organisational security measures implemented.

For data processors, the record must include the following information:

- the name and contact details of the processor and of each data controller on behalf of which the processor processes PII, and of the processor's representative and DPO;
- the categories of processing carried out on behalf of each data controller;
- a description of any transfers of PII to third countries and the safeguards relied upon; and
- a general description of the technical and organisational security measures implemented.

The DPA sets out several conditions for the processing of sensitive PII. To satisfy several of these conditions, data controllers must have an appropriate policy document in place. If a data controller processes sensitive PII under a condition that requires an appropriate policy document, the data controller must document the following information as part of its processing activities:

- the procedures for complying with the data protection principles in connection with the processing of the sensitive PII; and
- its policies as regards the retention and erasure of the sensitive PII, giving an indication of how long such sensitive PII is likely to be retained.

Data controllers must review and retain the policy document when processing the relevant sensitive PII, and then for at least six months afterwards. The policy document must also be made available on request to the ICO without charge.

Where an appropriate policy documentation is required, the data controller's records of processing activities under article 30 of the GDPR (as outlined above) must include:

- details of the relevant condition relied on, as set out in parts 1-3 of schedule 1 of the DPA;
- how processing satisfies article 6 of the GDPR (lawfulness of processing); and
- details of whether the sensitive PII is retained and erased in accordance with the appropriate policy documentation (and if not the reasons why not).

New processing regulations

24 | Are there any obligations in relation to new processing operations?

Data controllers are required to carry out a data protection impact assessment (DPIA) in relation to any processing of PII that is likely to result in a high risk to the rights and freedoms of natural persons. In particular, a DPIA is required in respect of any processing that involves:

- the systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing and on which decisions are made that produce legal effects concerning the natural person or that significantly affect the natural person;
- processing sensitive PII or PII relating to criminal convictions or offences on a large scale; or
- systematic monitoring of a publicly accessible area on a large scale.

A DPIA must be carried out in relation to all high-risk processing activities that meet the criteria above before the processing begins. The DPIA must include at least the following:

- a systematic description of the processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- an assessment of the proportionality and necessity of the processing in relation to the purposes;
- an assessment of the risks to the rights and freedoms of affected individuals; and
- information about the measures envisaged to address any risks to affected individuals (eg, safeguards, security measures, etc).

The GDPR also implements the concepts of 'data protection by design' and 'data protection by default'. In particular, this requires data controllers to implement appropriate technical and organisational measures in their processing systems to ensure that PII is processed in accordance with the GDPR, and to ensure that, by default, only PII that is necessary for each specific purpose is collected and processed. In addition, data controllers must ensure that by default PII is not made accessible to an indefinite number of persons without any intervention by the data subject.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

In the UK, data controllers are required to pay an annual registration fee to the Information Commissioner's Office (ICO). There is no obligation to do so if any of the following applies:

- no processing is carried out on a computer (or other automated equipment);
- the processing is performed solely for the maintenance of a public register;
- the data controller is a not-for-profit organisation, and the processing is only for the purposes of establishing or maintaining membership or support of that organisation; or
- the data controller only processes personally identifiable information (PII) for one or more of these purposes:
- staff administration;
- advertising, marketing and public relations;
- personal, family or household affairs;
- judicial functions; or
- accounts and records.

An entity that is a data processor only is not required to make this payment.

Formalities

26 | What are the formalities for registration?

There is a three-tier fee structure in the UK. Data controllers must pay a fee according to the following criteria:

- if the data controller has a maximum turnover of £632,000 or no more than 10 members of staff, £40;
- if the data controller has a maximum turnover of £36 million or no more than 250 members of staff, £60; or
- in all other cases, £2,900.

The data controller must include in the fee application its name, address, contact details of the person who is completing the fee registration and contact details of the data controller's data protection officer if it is required to appoint one, the number of staff members it has, the turnover for its financial year, and any other trading names it has. Data processors are not required to pay the registration fee.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

PII must not be processed unless the data controller has paid the required fee.

If the data controller has not paid a fee when required to do so or has not paid the correct fee, it may be subject to a fixed monetary penalty of 150 per cent of the highest charge payable by a data controller (ie, £4,350). As previously noted, an entity that is a data processor only (and not a data controller) is not required to register or pay the fee.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

On what grounds may the supervisory authority refuse to allow an entry on the register?

The ICO has no power to refuse the application provided that it is made in the prescribed form and includes the applicable fee.

Public access

29 | Is the register publicly available? How can it be accessed?

The fee register is publicly available, free of charge, from the ICO's website.

A copy of the register on DVD may also be requested by sending an email to accessICOinformation@ico.org.uk.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

An entry on the register does not cause the data controller to be subject to obligations or liabilities to which it would not otherwise be subject.

Other transparency duties

31 | Are there any other public transparency duties?

There are no additional public transparency duties.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Entities that provide outsourced processing services are typically 'data processors' under the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR). Data processors are subject to direct legal obligations under the DPA and GDPR in respect of the personally identifiable information (PII) that they process as outsourced service providers, but nevertheless data controllers are required to use only data processors that are capable of processing PII in accordance with the requirements of the DPA and the GDPR. The data controller must ensure that each data processor it selects offers sufficient guarantees that the relevant PII will be held with appropriate security measures and take steps to ensure that these guarantees are fulfilled. The data controller must also enter into a binding contract in writing with the data processor under which the data processor must be bound to:

- act only on the instructions of the data controller;
- ensure that persons that will process PII are subject to a confidentiality obligation;
- apply security controls and standards that meet those required by the GDPR;
- obtain general or specific authorisation before appointing any sub-processors, and ensure that any such sub-processors are bound by obligations equivalent to those imposed on the data processor;
- assist the data controller insofar as possible to comply with the data controller's obligation to respond to data subject rights requests;
- assist the data controller in relation to the obligations to notify personal data breaches and to carry out data protection impact assessments (and any required consultation with a supervisory authority);
- at the choice of the data controller, return the PII to the data controller or delete the PII at the end of the relationship;
- notify the data controller immediately if any instruction the data controller gives infringes the GDPR; and
- make available to the data controller all information necessary to demonstrate compliance with these obligations, and allow the data controller (or a third party nominated by the data controller) to carry out an audit.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

It is a criminal offence to knowingly or recklessly obtain or disclose PII without the consent of the data controller or procure the disclosure of PII to another party without the consent of the data controller. This prohibition is subject to a number of exceptions, such as where the action was taken for the purposes of preventing or detecting crime. The staff of the Information Commissioner's Office (ICO) are prohibited from disclosing PII obtained in the course of their functions other than in accord with those functions.

There are no other specific restrictions on the disclosure of PII, other than compliance with the general principles described earlier, and the cross-border restrictions.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII outside the European Economic Area (EEA) is prohibited unless that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals in relation to the processing of their PII.

Transfers are permitted where:

- the European Commission has made a finding in relation to the adequacy of PII protection of the country or territory;
- the European Commission has made a finding in relation to the relevant transfers; or
- one or more of the derogations applies.

The derogations include:

- where the data controller has the individual's explicit consent to the transfer;
- the transfer is necessary for a contract with the data subject;
- the transfer is necessary for legal proceedings;
- the transfer is necessary to protect the vital interest of the individual;
- the transfer is necessary for the purposes of the compelling legitimate interests pursued by the data controller; and
- the terms of the transfer have been approved by the ICO.

European Commission findings have been made in respect of the use of approved standard form model clauses for the export of PII and the adoption of a self-regulatory scheme in the US called the EU-US Privacy Shield, which replaced the Safe Harbor mechanism that was invalidated by the Court of Justice of the European Union in October 2015. However, on 16 July 2020, the Court of Justice of the European Union (CJEU) issued a landmark judgment in the Schrems II case (case C-311/18). In its judgment, the CJEU invalidated the EU-US Privacy Shield framework. Accordingly, organisations can no longer rely on the EU-US Privacy Shield framework to transfer PII from the EEA or UK to the US, and must find alternative mechanisms to transfer PII to the US. The Swiss-US Privacy Shield framework remains valid and can still be relied upon by organisations to transfer PII from Switzerland to the US. Entities within a single corporate group can enter into data transfer agreements known as 'binding corporate rules', which must be approved

by the supervisory authorities in the relevant European Union member states. In addition, an organisation can make a restricted transfer if it and the receiver have entered into a contract incorporating standard data protection clauses adopted by the European Commission. These are known as the 'standard contractual clauses'. They must be entered into by the data exporter (based in the European Economic Area) and the data importer (outside the EEA). While the EU-US Privacy Shield framework was invalidated, the CJEU decision concluded that standard contractual clauses are valid, provided the transferring organisation (the data exporter) determines that the country where the recipient organisation is located (the data importer) offers an 'adequate level of protection' to the personal data, as required by the GDPR.

Once the Brexit transition period ends, which is currently expected to be 31 December 2020, organisations may need to take additional steps to ensure their data transfers comply with the GDPR. The UK government has confirmed that transfers outside the UK to the EEA will not be restricted. As such, organisations that transfer PII from the UK to the EEA will still be able to do so and do not need to take any additional steps. However, organisations in the EEA that are transferring PII to the UK will need to take action to ensure the transfer of PII complies with the GDPR. In practice, this means that organisations transferring PII from the EEA to the UK will need to ensure the European Commission has made a finding in relation to the relevant transfers (eg, standard contractual clauses), or one or more of the derogations applies. The UK has confirmed that it will seek adequacy status to enable data flows between the EEA and the UK, but there is no guarantee that any adequacy decision will be in place prior to the end of the transition period.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Cross-border transfers do not require a specific notification to the ICO nor authorisation from the ICO.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on transfer apply equally to transfers to data processors and data controllers.

Onward transfers are taken into account in assessing whether adequate protection is provided in the receiving country. Onward transfers are covered in the European Commission-approved model clauses. Following the invalidation of the EU-US Privacy Shield framework in the Schrems II decision, organisations are no longer able to rely on the EU-US Privacy Shield framework to make onward transfers of PII.

Onward transfers are not controlled specifically where a transfer is made to a country that has been the subject of an adequacy finding by the European Commission. It would be anticipated that the law of the recipient country would deal with the legitimacy of the onward transfer.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to request access to personally identifiable information (PII) that relates to them. Within one month of receipt of a valid request, the data controller must confirm that it is or is not processing the individual's PII and, if it does so, provide a description of the PII, the purposes of the processing and recipients or categories of recipients of the PII, the relevant retention period for the PII, a description of the rights available to individuals under the General Data Protection Regulation (GDPR) and that the individual may complain to a supervisory authority and any information available to the data controller as to the sources of the PII, the existence of automated decision-making (including profiling), and the safeguards it provides if it transfers PII to a third country or international organisation. The data controller must also provide a copy of the PII in an intelligible form.

A data controller must be satisfied as to the identity of the individual making the request. A data controller does not have to provide third-party data where that would breach the privacy of the third party and may reject repeated identical requests, or charge a reasonable fee taking into account the administrative costs of providing the information.

In some cases the data controller may withhold PII to protect the individual (eg, where health data is involved, or to protect other important specified public interests such as the prevention of crime). All such exceptions are specifically delineated in the law.

In most cases the organisation cannot charge a fee to comply with a request for access. However, where the request is manifestly unfounded or excessive an organisation may charge a 'reasonable fee' for the administrative costs of complying with the request. A reasonable fee can also be charged if an individual requests further copies of their data following a request.

Other rights

38 | Do individuals have other substantive rights?

Individuals have the following further rights:

- to rectify PII that is inaccurate;
- to have PII erased in certain circumstances, for example, when the PII is no longer necessary for the purposes for which it was collected by the data controller;
- to restrict the processing of PII;
- to obtain a copy of PII in a structured, commonly used and machine-readable format, and to transmit that PII to a third-party data controller without hindrance, to the extent that it is technically feasible;
- to object to the processing of PII in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PII, except in particular circumstances.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to receive compensation if the individual suffers material or non-material damage as a result of the contravention of the GDPR by a data controller or data processor. The Data Protection Act 2018 (DPA) indicates that 'non-material' damage includes 'distress'.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals may take action in the courts to enforce any of their rights.

The Information Commissioner's Office (ICO) has no power to order the payment of compensation to individuals. Therefore, an individual who seeks compensation must take an action to the courts. All the other rights of individuals can be enforced by the ICO using its enforcement powers, including requiring the provision of information, and conducting audits.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The Data Protection Act 2018 (DPA), in accordance with the derogations permitted by the General Data Protection Regulation (GDPR), provides exemptions from certain obligations, including:

- exemptions from the obligations that limit the disclosure of personally identifiable information (PII);
- exemptions from the obligations to provide notice of uses of PII;
- exemptions from reporting personal data breaches;
- exemptions from complying with the data protection principles;
- exemptions from the rights of access; and
- exemptions from dealing with other individual rights.

The grounds for exemption include exemptions to protect freedom of expression, to protect national security and policing, to support legal privilege, to protect the actions of regulatory authorities and to protect the collection of taxes and the position of the armed forces.

Exemptions also apply to protect individuals who may be vulnerable, such as those who are suffering from mental illness.

Further exemptions apply where the PII is made publicly available under other provisions.

Specific exemptions apply to allow the retention and use of PII for the purposes of research. Exemptions are also available under the DPA for crime, law and public protection, and finance, management and negotiations.

All exemptions are limited in scope and most apply only on a case-by-case basis.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data controllers may appeal orders of the Information Commissioner's Office (ICO) to the General Regulatory Chamber (First-tier Tribunal). Appeals must be made within 28 days of the ICO notice and must state the full reasons and grounds for the appeal (ie, that the order is not in accordance with the law or the ICO should have exercised its discretion differently).

Appeals against decisions of the General Regulatory Chamber (First-tier Tribunal) can be made (on points of law only) to the Administrative Appeals Chamber of the Upper Tribunal, appeals from which may be made to the Court of Appeal.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

It is unlawful to store information (such as a cookie) on a user's device, or gain access to such information, unless the user is provided with clear and comprehensive information about the storage of, and access to, that information, and has provided his or her consent. Consent must be validly obtained in accordance with the requirements of the General Data Protection Regulation (GDPR). Such consent is not, however, required where the information is:

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@huntonak.com

James Henderson
jhenderson@huntonak.com

Jonathan Wright
wrightj@huntonak.com

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

- used only for the transmission of communications over electronic communications networks; or
- strictly necessary for the provision of a service requested by the user.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

It is unlawful to send unsolicited electronic marketing (ie, via technologies such as SMS, fax or email) unless the opt-in consent of the recipient has been obtained. However, an unsolicited marketing email may be sent to a recipient whose contact details were obtained in the course of a sale, or negotiation of sale, of a product or service, provided that the unsolicited marketing relates to similar products or services, the recipient is given a simple and free-of-charge means to opt out of receiving such marketing at the point their information is collected, and in all subsequent marketing communications (and has not yet opted out). Any consent obtained must comply with the GDPR's consent requirements.

It is generally permissible to make unsolicited telephone marketing calls, unless the recipient has previously notified the caller that he or she does not wish to receive such calls or the recipient's phone number is listed on the directory of subscribers that do not wish to receive such calls (known as the Telephone Preference Service). Any individuals may apply to have their telephone number listed in this directory. Separate requirements and separate rules around marketing to corporate subscribers (ie, an individual in his or her professional capacity) apply, and will need to be considered for business-to-business marketing.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules or legislation that govern the processing of personally identifiable information (PII) through cloud computing, and such processing must be compliant with the Data Protection Act 2018 (DPA). The ICO has released guidance on the subject of cloud computing, which discusses the identity of data controllers and data processors in the context of cloud computing, as well as the need for written contracts, security assessments, compliance with the DPA and the use of cloud

providers from outside the UK. This guidance was published under the old law (ie, Data Protection Act 1998). The Information Commissioner's Office (ICO) has confirmed that, while much of the guidance remains relevant, it intends to update the guidance in line with the GDPR.

UPDATE AND TRENDS

Key developments of the past year

46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There are no updates at this time.

United States

Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The United States' legislative framework for the protection of PII historically has resembled a patchwork quilt. Unlike other jurisdictions, the US does not have a single dedicated data protection law at the federal level, but instead regulates privacy primarily by industry, on a sector-by-sector basis. There are numerous sources of privacy law in the US, including laws and regulations developed at both the federal and state levels. These laws and regulations may be enforced by federal and state authorities, and many provide individuals with a private right to bring lawsuits against organisations they believe are violating the law. Starting in 2018, increased legislative activity at the state level signalled a shift in focus toward more broad-based consumer privacy legislation in the United States. California became the first state to enact such legislation with the passage of the California Consumer Privacy Act (CCPA), a broad privacy law inspired in part by the General Data Protection Regulation (GDPR) in the European Union that is aimed at protecting personal information of consumers across industries. Since then, numerous other states have proposed similarly broad privacy legislation, while multiple comprehensive privacy bills have been introduced at the federal level in the US Congress.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no single regulatory authority dedicated to overseeing data protection law in the US. At the federal level, the regulatory authority responsible for oversight depends on the law or regulation in question. In the financial services context, for example, the Consumer Financial Protection Bureau and various financial services regulators (as well as state insurance regulators) have adopted standards pursuant to the Gramm-Leach-Bliley Act (GLB) that dictate how firms subject to their regulation may collect, use and disclose non-public personal information. Similarly, in the healthcare context, the Department of Health and Human Services is responsible for enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Outside of the regulated industries context, the Federal Trade Commission (FTC) is the primary federal privacy regulator in the US. Section 5 of the FTC Act, which is a general consumer protection law that prohibits 'unfair or deceptive acts or practices in or affecting commerce', is the FTC's primary enforcement tool in the privacy arena. The FTC has used its authority under section 5 to bring numerous privacy enforcement actions for a wide range of alleged violations by entities whose information practices have been deemed 'deceptive' or 'unfair'. Although section 5 does not give the FTC fining authority, it does enable it to bring enforcement actions against alleged violators, and these enforcement actions typically have resulted in consent decrees that prohibit the company from future misconduct and often require audits biennially for up to 20 years. Under section 5, the FTC is able to fine businesses that have violated a consent order.

At the state level, attorneys general also have the ability to bring enforcement actions for unfair or deceptive trade practices, or to enforce violations of specific state privacy laws. The California attorney general, for example, will be empowered to enforce violations of the CCPA. Some state privacy laws allow affected individuals to bring lawsuits to enforce violations of the law

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There are no regulations or structures that require the various federal and state data protection authorities to cooperate with one another. In the event of a data breach, however, many state attorneys general set up multistate task forces to pool resources, investigate the companies that experienced the breach, and reach a settlement or collectively litigate against the company. The resolutions often require companies to improve their information security programmes and obtain third-party assessments of their programmes.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

In general, violations of federal and state privacy laws lead to civil, not criminal, penalties. The main exceptions are the laws directed at surveillance activities and computer crimes. Violations of the federal Electronic Communications Privacy Act (which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act) or the Computer Fraud and Abuse Act can lead to criminal sanctions and civil liability. In addition, many states have enacted surveillance laws that include criminal sanctions, in addition to civil liability, for violations.

Outside of the surveillance context, the US Department of Justice is authorised to criminally prosecute serious HIPAA violations. In circumstances where an individual knowingly violates restrictions on obtaining and disclosing legally cognisable health information, the Department of Justice may pursue criminal sanctions

SCOPE

Exempt sectors and institutions

5 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

There is no single regulatory authority dedicated to overseeing data protection law in the United States. At the federal level, different privacy requirements apply to different industry sectors and data processing activities. These laws often are narrowly tailored and address specific data uses. For those entities not subject to industry-specific regulatory authority, the Federal Trade Commission (FTC) has broad enforcement authority at the federal level, and attorneys general at the state level, to bring enforcement action for unfair or deceptive trade practices in the privacy context.

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications is regulated primarily at the federal level by the Electronic Communications Privacy Act, which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act. The federal Computer Fraud and Abuse Act also prohibits certain surveillance activities, but is focused primarily on restricting other computer-related activities pertaining to hacking and computer trespass. At the state level, most states have laws that regulate the interception of communications.

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question. Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM. Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities. Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC. Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

Other laws

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

In addition to the laws set forth above, there are numerous other federal and state laws that address privacy issues, including state information security laws and laws that apply to:

- consumer report information: Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act of 2003;
- children's information: Children's Online Privacy Protection Act;
- driver's information: Driver's Privacy Protection Act of 1994;
- video rental records: Video Privacy Protection Act; and
- federal government activities: Privacy Act of 1974.

The Cybersecurity Information Sharing Act (CISA) authorises entities to engage in certain cybersecurity monitoring, defence practices and information-sharing activities for purposes of protecting against cybersecurity threats. To help companies secure their information and systems, CISA provides businesses with certain liability protections in connection with monitoring information systems for cybersecurity purposes, implementing cybersecurity defensive measures, and sharing cyber intelligence with other private entities and federal government agencies.

In 2018, the California legislature enacted the California Consumer Privacy Act (CCPA), which became effective on 1 January 2020. The Act applies to any for-profit business that:

- does business in California;
- collects consumers' personal information (or on whose behalf such information is collected);
- alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; and
- satisfies certain revenue thresholds or collects the personal information of 50,000 or more consumers, households or devices.

The CCPA defines 'personal information' broadly and contains provisions granting California consumers certain rights with respect to their personal information. This new legislation in California has helped set the stage for a number of similar proposed laws currently pending in various state legislatures across the US, as well as a possible federal data privacy law.

PII formats

8 What forms of PII are covered by the law?

The US does not have a dedicated data protection law. Thus, the definition of personally identifiable information (PII) varies depending on the underlying law or regulation. In the state security breach notification law context, for example, the definition of PII generally includes an individual's name plus his or her social security number, driver's licence number, or financial account number. Some states broaden the definition of PII under the data breach notification laws to include elements such as medical information, insurance information, biometrics, email addresses and passwords to online accounts. In other contexts, such as FTC enforcement actions, Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act of 1996, the definition of PII is much broader. Although certain laws apply only to electronic PII, many cover PII in any medium, including hard copy records.

The CCPA contains a broad definition of PII that includes any 'information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household'.

Extraterritoriality

9 Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

As a general matter, the reach of US privacy laws is limited to organisations that are subject to the jurisdiction of US courts as constrained by constitutional due process considerations. Determinations regarding such jurisdiction are highly fact-specific and depend on the details of an organisation's contacts with the US.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Generally, US privacy laws apply to all processing of PII. There are no formal designations of 'controllers' and 'processors' under US law as there are in the laws of other jurisdictions. There are, however, specific

laws that set forth different obligations based on whether an organisation would be considered a data owner or a service provider. The most prominent example of this distinction is found in the US state breach notification laws. Pursuant to these laws, it is generally the case that the owner of the PII is responsible for notifying affected individuals of a breach, whereas a service provider is responsible for informing the data owner that it has suffered a breach affecting the data owner's data. Once a data owner has been notified of a breach by a service provider, the data owner, not the service provider, then must notify affected individuals.

The CCPA has adopted a concept quite similar to the controller concept under the General Data Protection Regulation, in that businesses directly subject to the law are defined to mean those entities who determine the purposes and means of the processing of consumers' personal Information.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

US privacy laws generally do not limit the retention of personally identifiable information (PII) to certain specified grounds. There are, however, laws that may indirectly affect an organisation's ability to retain PII. For example, organisations that are collecting personal information online from California residents must comply with the California Online Privacy Protection Act. Pursuant to this law, and general consumer expectations in the US, the organisation must provide a privacy notice detailing the PII the company collects and how it is used. If the organisation uses the PII in materially different ways than those set forth in the privacy notice without providing notice and obtaining consent for such uses from the relevant consumers, these uses would likely be considered a deceptive trade practice under federal and state unfair competition laws. Similar laws are in place in Delaware and Nevada.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

Since the United States does not have a dedicated data protection law, there is no singular concept of 'sensitive data' that is subject to heightened standards. There are, however, certain types of information that generally are subject to more stringent rules, which are described below.

Sensitive data in the security breach notification context

To the extent an organisation maintains individuals' names plus their social security numbers, driver's licence numbers or financial account numbers, notification generally is required under state and federal breach notification laws to the extent the information has been acquired or accessed by an unauthorised third party. Some states include additional data elements that could trigger breach notification. These include medical information, insurance information, biometrics, email addresses, and passwords to online accounts.

Consumer report information

The Fair Credit Reporting Act (FCRA) seeks to protect the confidentiality of information bearing on the creditworthiness and standing of consumers. The FCRA limits the permissible purposes for which reports that contain such information (known as consumer reports) may be disseminated, and consumer reporting agencies must verify that anyone requesting a consumer report has a permissible purpose for receiving the report.

Background screening information

Many sources of information used in background checks are considered public records in the US, including criminal, civil court, bankruptcy, tax lien, professional licensing, workers' compensation and driving records. The FCRA imposes restrictions on the inclusion of certain public records in background screening reports when performed by consumer reporting agencies. Employers also can investigate job applicants and employees using internet search engines, but they must comply with their legal obligations under various labour and employment laws to the extent such laws restrict the use of the information. For instance, consideration of factors such as age, race, religion, disability, or political or union affiliation in making employment decisions can be the basis for a claim of unlawful discrimination under federal or state law.

Health information

Health Insurance Portability and Accountability Act of 1996 (HIPAA) specifies permissible uses and disclosures of protected health information (PHI), mandates that HIPAA-covered entities provide individuals with a privacy notice and other rights, regulates covered entities' use of service providers (known as business associates), and sets forth extensive information security safeguards relevant to electronic PHI.

Children's information

Children's Online Privacy Protection Act (COPPA) imposes extensive obligations on organisations that collect personal information from children under 13 years of age online. COPPA's purpose is to provide parents and legal guardians greater control over the online collection, retention and disclosure of information about their children.

Under the Privacy Rights for California Minors in the Digital World law, California minors who are registered users of a website, online service or mobile application may seek the removal of content and information that the minors have posted. A 'minor' is defined as a California resident under the age of 18.

The California Consumer Privacy Act of 2018 prohibits a business from selling a minor's personal information unless:

- the consumer is between 13 and 16 years of age and has affirmatively authorised the sale (ie, they opt in); or
- the consumer is less than 13 years of age and the consumer's parent or guardian has affirmatively authorised the sale.

Biometric information

Illinois, Texas and Washington have enacted biometric privacy laws that set forth requirements for businesses that collect and use biometric information for commercial purposes. These laws generally require that companies must provide notice to individuals and obtain their affirmative consent before using their biometric identifiers for commercial purposes. The laws also require companies to implement security measures to protect the biometric information they maintain and to retain the biometric identifiers for no longer than necessary to comply with the law, protect against fraud, criminal activity, security threats or liability, or to provide the service for which the biometric identifier was collected.

State social security number laws

Numerous state laws impose obligations with respect to the processing of state social security numbers (SSNs). These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on identity cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions, unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

A number of state laws also impose restrictions targeting specific SSN uses.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

For organisations not otherwise subject to specific regulation, the primary law requiring them to provide a privacy notice to consumers is California Online Privacy Protection Act. This law requires a notice when an organisation collects personal information from individuals in the online and mobile contexts. The law requires organisations to specify in the notice:

- the categories of personally identifiable information (PII) collected through the website;
- the categories of third-party persons or entities with whom the operator may share the PII;
- the process an individual must follow to review and request changes to any of his or her PII collected online, to the extent such a process exists;
- how the operator responds to web browser 'do-not-track' signals or similar mechanisms that permit individuals to exercise choice regarding the collection of their PII online over time and across third-party websites or online services, if the operator engages in such collection;
- whether third parties collect PII about individuals' online activities over time and across different websites when an individual uses the operator's website or online service;
- the process by which consumers who visit the website or online service are notified of material changes to the privacy notice for that website; and
- the privacy notice's effective date.

Delaware and Nevada have also enacted laws that require operators of commercial internet services to provide similar information to their users when collecting PII online.

The California Consumer Privacy Act (CCPA) also imposes specific privacy notice disclosure requirements, which apply to personal information collected both online and offline. For example, businesses must provide notice to consumers of their rights under the CCPA (eg, the right to opt out of the sale of personal information) and how to exercise those rights. The CCPA also requires a business to include the following in its privacy notice:

- a list of the categories of personal information collected about consumers in the preceding 12 months;
- the categories of sources from which the personal information was collected;
- the business or commercial purpose for collecting or selling the information;
- the categories of third parties with whom the personal information is shared; and
- lists of the categories of personal information sold and disclosed about consumers, if the business sells consumers' personal information or discloses it to third parties for a business purpose.

If the business sells personal information, it must provide a clear and conspicuous link on their website that says 'Do not sell my personal information' and provide consumers with a mechanism to opt out of the sale of their personal information, a decision the business must respect. Companies must update their notices at least once every 12 months. The CCPA also imposes a limited notice obligation in the employment context.

In addition to the California, Delaware and Nevada laws, there are other federal laws that require a privacy notice to be provided in certain circumstances, such as the following.

Children's Online Privacy Protection Act

Pursuant to the Children's Online Privacy Protection Rule of the Federal Trade Commission (FTC), implemented pursuant to Children's Online Privacy Protection Act (COPPA), operators of websites or online services that are directed to children under 13 years old, or who knowingly collect information from children online, must provide a conspicuous privacy notice on their site. The notice must include statutorily prescribed information, such as the types of personal information collected, how the operator will use the personal information, how the operator may disclose the personal information to third parties, and details regarding a parent's ability to review the information collected about a child and opt out of further information collection and use. In most cases, an operator that collects information from children online also must send a direct notice to parents that contains the information set forth above along with a statement that informs parents the operator intends to collect the personal information from their child. The operator also must obtain verifiable parental consent prior to collecting, using or disclosing personal information from children.

Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act

The Fair Credit Reporting Act (FCRA), as amended by Fair and Accurate Credit Transactions Act of 2003 (FACTA), imposes several requirements on consumer reporting agencies to provide consumers with notices, including in the context of written disclosures made to consumers by a consumer reporting agency, identity theft, employment screening, pre-screened offers of credit or insurance, information sharing with affiliates, and adverse actions taken on the basis of a consumer report.

Gramm-Leach-Bliley Act

Financial institutions must provide an initial privacy notice to customers by the time the customer relationship is established. If the financial institution shares non-public personal information with non-affiliated third parties outside of an enumerated exception, the entity must provide each relevant customer with an opportunity to opt out of the information sharing. Following this initial notice, financial institutions subject to Gramm-Leach-Bliley Act (GLB) must provide customers with an annual notice. The annual notice is a copy of the full privacy notice and must be provided to customers each year for as long as the customer relationship persists. For 'consumers' (individuals that have obtained a financial product or service for personal, family or household purposes but do not have an ongoing, continuing relationship with the financial institution), a notice generally must be provided before the financial institution shares the individual's non-public personal information with third parties outside of an enumerated exception. A GLB privacy notice must explain what non-public personal information is collected, the types of entities with whom the information is shared, how the information is used, and how it is protected. The notice also must indicate the consumer's right to opt out of certain information sharing with non-affiliated parties. In 2009, the federal financial regulators responsible for enforcing privacy regulations implemented pursuant to GLB released model forms for financial institutions to use when developing their privacy notices. Financial institutions that use the model form in a manner consistent with the regulators' published instructions are deemed compliant with the regulation's notice requirements. In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act transferred GLB privacy notice rule-making authority from the financial regulatory agencies to the Consumer Financial Protection

Bureau (CFPB). The CFPB then restated the GLB implementing regulations, including those pertaining to the model form, in Regulation P.

Health Insurance Portability and Accountability Act

The Privacy Rule promulgated pursuant to Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities to provide individuals with a notice of privacy practices. The Rule imposes several content requirements, including:

- the covered entities' permissible uses and disclosures of protected health information (PHI);
- the individual's rights with respect to the PHI and how those rights may be exercised;
- a list of the covered entity's statutorily prescribed duties with respect to the PHI; and
- contact information for the individual at the covered entity responsible for addressing complaints regarding the handling of PHI.

Exemption from notification

14 | When is notice not required?

Notice would not be required if a business is subject to specifically regulated scenarios.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

In the regulated contexts discussed above, individuals are provided with limited choices regarding the use of their information. The choices are dependent upon the underlying law. Under GLB, for example, customers and consumers have a legal right to opt out of having their non-public personal information shared by a financial institution with third parties (outside an enumerated exception). Similarly, under the FCRA, as amended by FACTA, individuals have a right to opt out of having certain consumer report information shared by a consumer reporting agency with an affiliate, in addition to another opt-out opportunity prior to any use of a broader set of consumer report information by an affiliate for marketing reasons. Federal telemarketing laws and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 Act give individuals the right to opt out of receiving certain types of communications, as do similar state laws.

In addition, California's Shine the Light Law requires companies that collect personal information from residents of California generally to either provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the preceding calendar year or, alternatively, to give the individuals the right to opt out of such third-party sharing. This right is expanded in the CCPA, which provides that, upon request from a California consumer, an organisation must disclose:

- the categories and specific pieces of personal information the business has collected about the consumer;
- the categories of sources from which the personal information is collected;
- the business or commercial purposes for collecting or selling personal information;
- the categories of third parties with whom the business shares personal information;
- if applicable, the categories of personal information about the consumer the business has disclosed for a business purpose and the categories of third parties to whom each category of personal information was disclosed; and
- if applicable, the categories of personal information about the consumer the business has sold and the categories of third parties to whom each category of personal information was sold.

Under the CCPA, a consumer also has the right to request that a business delete any personal information about the consumer, which the business has collected from the consumer. The CCPA also provides consumers with the right to opt out of the sale of their personal information.

As the primary regulator of privacy issues in the US, the FTC periodically issues guidance on pressing issues. In the FTC's 2012 report entitled 'Protecting Consumer Privacy in an Era of Rapid Change', the FTC set forth guidance indicating that organisations should provide consumers with choices with regard to uses of personal information that are inconsistent with the context of the interaction through which the organisation obtained the personal information. In circumstances where the use of the information is consistent with the context of the transaction, the FTC indicated that offering such choices is not necessary.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

There is no law of general application in the US that imposes standards related to the quality, currency and accuracy of PII. There are laws, however, in specific contexts that contain standards intended to ensure the integrity of personal information maintained by an organisation. The FCRA, for example, requires users of consumer reports to provide consumers with notices if the user will be taking an adverse action against the consumer based on information contained in a consumer report. These adverse action notices must provide the consumer with information about the consumer's right to obtain a copy of the consumer report used in making the adverse decision and to dispute the accuracy or completeness of the underlying consumer report. Similarly, pursuant to the HIPAA Security Rule, covered entities must ensure, among other things, the integrity of electronic PHI.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

US privacy laws generally do not impose direct restrictions on an organisation's retention of personal information. There are, however, thousands of records retention laws at the federal and state level that impose specific obligations on how long an organisation may (or must) retain records, many of which cover records that contain personal information.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

US privacy laws have not specifically adopted the finality principle. As a practical matter, organisations typically describe their uses of personal information collected from consumers in their privacy notices. To the extent an organisation uses the personal information it collects subject to such a privacy notice for materially different purposes than those set forth in the notice, it is likely that such a practice would be considered a deceptive trade practice under federal and state consumer protection laws.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

In the US, organisations must use the personal information they collect in a manner that is consistent with any privacy representations it has made in their privacy notices or otherwise. To the extent an organisation would like to use previously collected personal information for a materially different purpose, the FTC and state attorneys general would expect the organisation to first obtain opt-in consent from the consumer for such use. Where the privacy notice is required by a statute (eg, a notice to parents pursuant to COPPA), failure to handle the PII as described pursuant to such notice also may constitute a violation of the statute.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Similar to privacy regulation, there is no comprehensive federal information security law in the US. Accordingly, the security obligations that are imposed on data owners and entities that process personally identifiable information (PII) on their behalf depend on the regulatory context. These security obligations include:

Gramm-Leach-Bliley Act

The Safeguards Rule implemented pursuant to the Gramm-Leach-Bliley Act (GLB) requires financial institutions to 'develop, implement, and maintain a comprehensive information security program' that contains administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of customer information. The requirements of the Safeguards Rule apply to all non-public personal information in a financial institution's possession, including information about the institution's customers as well as customers of other financial institutions. Although the Safeguards Rule is not prescriptive in nature, it does set forth five key elements of a comprehensive information security programme:

- designation of one or more employees to coordinate the programme;
- conducting risk assessments;
- implementation of safeguards to address risks identified in risk assessments;
- oversight of service providers; and
- evaluation and revision of the programme in light of material changes to the financial institution's business.

Health Insurance Portability and Accountability Act

The Security Rule implemented pursuant to Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to electronic protected health information (ePHI), sets forth specific steps that covered entities and their service providers must take to:

- ensure the confidentiality, integrity, and availability of ePHI;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- protect against any reasonably anticipated uses or disclosures of ePHI; and
- ensure compliance with the Security Rule by the covered entity's workforce.

Unlike other US information security laws, the Security Rule is highly prescriptive and sets forth detailed administrative, technical and physical safeguards.

State information security laws

Laws in several US states, including California, impose general information security standards on organisations that maintain personal information. California's law, for example, requires organisations that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorised access, destruction, use, modification or disclosure. In addition, organisations that disclose personal information to non-affiliated third parties must contractually require those entities to maintain reasonable security procedures.

Massachusetts Standards for the Protection of Personal Information

In 2008, Massachusetts issued regulations requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive, written information security programme to protect the data. The regulations apply in the context of both consumer and employee information, and require the protection of personal data in both paper and electronic formats. Unlike the California law, the Massachusetts law contains certain specific data security standards, including required technical safeguards, on all private entities with Massachusetts consumers or employees.

New York SHIELD Act

In 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended the state's existing data breach notification law to impose certain data security requirements on businesses that own or license computerised data that includes New York residents' 'private information.' The SHIELD Act requires businesses to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information including, but not limited to, the disposal of such data. A business can comply with the SHIELD Act's 'reasonable safeguards' requirement by either being subject to and compliant with applicable federal or New York data security rules, regulations or statutes or implementing a data security program that includes reasonable administrative, technical and physical safeguards.

New York Department of Financial Services Cybersecurity Regulation

In 2017, the New York State Department of Financial Services (NYDFS) issued a regulation that establishes a robust set of cybersecurity requirements for financial services providers regulated by the NYDFS. The cybersecurity regulation applies to entities that operate under a NYDFS licence, registration or charter pursuant to New York banking, insurance or financial services law. The cybersecurity regulation requires such covered entities to maintain a comprehensive cybersecurity programme and implement certain processes and technical controls related to risk assessments, user access privileges, software security, system auditing and monitoring, data encryption, data disposal and retention, and cybersecurity incident response. In addition, the regulation assigns cybersecurity oversight responsibilities to senior officials and boards of directors and requires entities to report cybersecurity events to the NYDFS.

Nevada encryption law

Nevada law requires that organisations doing business in Nevada and that accept payment cards must comply with the Payment Card Industry Data Security Standard (PCI DSS). It requires that other organisations doing business in Nevada use encryption when transferring 'any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data collector', and moving 'any data storage device containing personal

information beyond the logical or physical controls of the data collector or its data storage contractor'.

State social security number laws

Numerous state laws impose obligations with respect to the processing of state social security numbers (SSNs). These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on ID cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

A number of state laws also impose restrictions targeting specific SSN uses.

Key industry and government standards

There are several key industry standards in the area of information security. The PCI DSS applies to all entities that process credit or debit cards. It obligates covered entities to comply with prescriptive information security requirements, which include:

- installing and maintaining a firewall configuration to protect cardholder data;
- encrypting transmission of cardholder data across public networks;
- protecting systems against malware and regularly updating anti-virus software or programs; and
- restricting physical access to cardholder data.

Entities subject to the PCI DSS are required to validate their compliance on an annual basis. The specific requirements necessary to certify compliance depend on the type of entity involved in the processing of payment cards and the number of payment cards processed by the covered entity pursuant to each payment card brand's compliance validation programme.

The National Institute of Standards and Technology (NIST), which is part of the US Department of Commerce, has produced various publications and guidance on a host of information security topics that are intended to help businesses. The most significant of the NIST security publications is the NIST Cybersecurity Framework. This is a flexible document that gives users the discretion to decide which aspects of network security to prioritise, what level of security to adopt and which standards, if any, to apply. Other guidance documents address methods of media sanitisation, conducting risk assessments, security considerations in the information system development life cycle and storage encryption for end user devices.

In addition, the International Organization for Standardization (ISO) is a non-governmental organisation composed of the national standards institutes of 161 countries. The ISO sets international standards across a range of industries. In the area of information security, the ISO has promulgated two important standards: 27001 and 17799/27002. ISO 27001 provides a 'process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system'. It is a flexible standard, and users are encouraged to:

- understand their information security requirements and the need to establish policy objectives for information;
- implement controls to manage information security risks in the context of the organisation's overall business risks;
- monitor and review the performance and effectiveness of the Information Security Management System; and
- continually improve the Information Security Management System based on objective measurement.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There are no breach notification laws of general application at the federal level. There are, however, numerous targeted breach notification laws at both the state and federal level, including:

State breach laws

At present, all 50 states, the District of Columbia, the US Virgin Islands, Guam and Puerto Rico have enacted breach notification laws that require data owners to notify affected individuals in the event of unauthorised access to or acquisition of personal information, as that term is defined in each law. In addition to notification of individuals, a majority of the state laws also require notice to a state regulator in the event of a breach, typically the state attorney general. Although most state breach laws require notification only if there is a reasonable likelihood that the breach will result in harm to affected individuals, a number of jurisdictions do not employ such a harm threshold and require notification of any incident that meets their definition of a breach.

Federal interagency guidance

Several federal banking regulators issued the Interagency Guidance on Response Programs for Unauthorised Access to Customer Information and Customer Notice. Entities regulated by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision are subject to the Interagency Guidance. The Interagency Guidance sets forth that subject financial institutions develop and implement a response programme to address incidents of unauthorised access to customer information processed in systems the institutions or their service providers use to access, collect, store, use, transmit, protect, or dispose of the information. In addition, the Interagency Guidance contains three key breach notification requirements. First, when a financial institution becomes aware of an incident involving unauthorised access to or use of sensitive customer information, the institution must promptly notify its primary federal regulator. Second, the institution must notify appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention. Third, the institution also must notify relevant customers of the incident if the institution's investigation determines that misuse of sensitive customer information has occurred or is reasonably possible. In this context, 'sensitive customer information' means a customer's name, address, or telephone number in conjunction with the customer's SSN, driver's licence number, account number, credit or debit card number, or a PIN or password that would permit access to the customer's account. Any combination of these data elements that would allow an unauthorised individual to access the customer's account also would constitute sensitive customer information.

Health Information Technology for Economic and Clinical Health Act

The information security breach provisions in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) apply in the healthcare context, governing both HIPAA-covered entities and non-HIPAA covered entities. The HITECH Act and the breach-related provisions of the Department of Health and Human Services regulations implementing the Act require HIPAA-covered entities that experience an information security breach to notify affected individuals, and service providers of HIPAA-covered entities to notify the HIPAA-covered entity following the discovery of a breach. Unlike the state breach notification

laws, the obligation to notify as a result of an information security breach under the HITECH Act falls on any HIPAA covered entity that 'accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured [personal health information (PHI)]'. Any HIPAA-covered entity that processes unsecured PHI must notify affected individuals in the event of a breach, whether the covered entity owns the data or not.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No, the appointment of a data protection officer is not mandatory under the privacy rules of general application. Many organisations in the US appoint a chief privacy officer (CPO), but his or her responsibilities are dictated by business need rather than legal requirements. Certain sector-specific laws do require the appointment of a CPO. For example, Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the appointment of a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. In addition, several federal and state laws require that a chief information security officer or an equivalent be appointed. These laws include the Gramm-Leach-Bliley Act (GLB), HIPAA and the New York State Department of Financial Services' Cybersecurity Regulations.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

There are currently no legal requirements of general application that obligate owners of personally identifiable information (PII) to maintain internal records or establish internal processes or documentation. There are several statutory frameworks in the US that require organisations to develop an information security programme, which typically must contain internal processes and documentation. These include requirements imposed by GLB, HIPAA and state information security laws.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

Generally, there are no legal obligations in relation to new processing operations, such as to apply a privacy-by-design approach or carry out privacy impact assessments. Applicable to US federal agencies only, the E-Government Act of 2002 requires the completion and publication of privacy impact assessments when the agency engages in a new collection of, or applies new technologies to, personally identifiable information. The Federal Trade Commission issued a report, however, that recommends that companies consider privacy-by-design principles during all stages of the design and development of products and services.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no registration requirements for data processing activities in the US.

Formalities

26 | What are the formalities for registration?

There are no registration requirements for data processing activities in the US.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There are no registration requirements for data processing activities in the US.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

There are no registration requirements for data processing activities in the US.

Public access

29 | Is the register publicly available? How can it be accessed?

There are no registration requirements for data processing activities in the US.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

There are no registration requirements for data processing activities in the US.

Other transparency duties

31 | Are there any other public transparency duties?

There are no other public transparency duties.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

As a general matter, organisations address privacy and information security concerns in their agreements with service providers that will provide outsourced processing services. There are no laws of general application in the US that impose requirements on data owners with respect to their service providers. There are, however, specific laws that address this issue, such as the following.

Health Insurance Portability and Accountability Act

Through the Privacy and Security Rules, Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes significant restrictions on the disclosure of PHI. The regulations require covered entities to enter into business associate agreements containing statutorily mandated language before PHI may be disclosed to a service provider.

Gramm-Leach-Bliley Act

In accordance with the Privacy Rule enacted pursuant to Gramm-Leach-Bliley Act (GLB), prior to disclosing consumer non-public personal information to a service provider, a financial institution must enter into a contract with the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes

for which the information was disclosed. Under the Safeguards Rule enacted pursuant to GLB, prior to allowing a service provider access to customer personal information, the financial institution must take reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards, and require the service provider by contract to implement and maintain such safeguards.

State information security laws

A number of states impose a general information security standard on businesses that maintain personal information. These states have laws requiring companies to implement reasonable information security measures. California law and Massachusetts law require organisations that disclose personal information to service providers to include contractual obligations that those entities maintain reasonable security procedures. The California Consumer Privacy Act (CCPA) prescribes additional content to be included in contracts with service providers.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

A wide variety of laws contain disclosure restrictions targeted to specific forms of personally identifiable information (PII). For example, HIPAA and GLB impose limitations on certain disclosures, such as requirements for consent and for contracts with certain types of recipients. The CCPA provides rights to consumers with respect to a business's ability to sell their personal information to certain types of third parties.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

US privacy laws do not impose restrictions on cross-border data transfers.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

US privacy laws do not impose restrictions on cross-border data transfers.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

US privacy laws do not impose restrictions on cross-border data transfers.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

There are no laws of general application in the United States that provide individuals with a right to access the personal information about them that is held by an organisation. There are specific laws that address access rights, such as the following.

Health Insurance Portability and Accountability Act

Under the Privacy Rule enacted pursuant to Health Insurance Portability and Accountability Act of 1996, an individual has a right to access protected health information (PHI) about the individual that is maintained by the covered entity unless the covered entity has a valid reason for denying the individual such access. Valid reasons can include the fact that the PHI is subject to restricted access under other laws, or that access to the PHI is reasonably likely to cause substantial harm to another person. A covered entity must provide the requested access to the PHI within 30 days of the request and must explain the justification for any denial of access.

California's Shine the Light Law

Under this law, organisations that collect personal information from California residents generally must either:

1 provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the prior calendar year; or
2 allow such individuals the right to opt out of most third-party sharing.

If an organisation implements option (1), it must provide California residents with a postal address, email address or toll-free telephone or fax number that California residents may contact to obtain the list of relevant third parties. Organisations are required to respond only to a single request per California resident per calendar year.

California Consumer Privacy Act

Under this law, California consumers have a right to request information about the personally identifiable information (PII) organisations collected, shared and sold within the past 12 months. Specifically, a consumer has a right to request that an organisation disclose:

1 the categories of PII the organisation has collected about that consumer;
2 the categories of sources from which the PII is collected;
3 the business or commercial purpose for collecting or selling PII;
4 the categories of third parties with whom the organisation shares PII;
5 the specific pieces of PII it has collected about that consumer;
6 the categories of PII it has sold about the consumer and the categories of third parties to whom the PII was sold; and
7 the categories of PII that the organisation disclosed for a business purpose and the categories of third parties to whom the PII was disclosed for a business purpose.

The California Consumer Privacy Act (CCPA) also provides that an organisation's response to an access request must be delivered in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.

Other rights

38 | Do individuals have other substantive rights?

The CCPA provides consumers with the right to delete the personal information that the business has collected about the consumer and direct any service providers to delete the consumer's personal information. There are several enumerated exceptions to this deletion requirement, such as if it is necessary to maintain the consumer's personal information to complete the transaction for which the personal information was collected or to protect against malicious, deceptive, fraudulent or illegal activity.

In addition, some sector-specific laws provide other substantive rights. For example, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 provides individuals with the right to amend their PHI. If an individual requests that a covered entity amend the individual's PHI, the covered entity must do so within 60 days of the request and must explain any reasons for denying the request. The

Children's Online Privacy Protection Act allows parents or legal guardians to revoke their consent and refuse the further use or collection of personal information from their child. This law also allows parents or guardians to request deletion of their child's personal information. The Fair Credit Reporting Act (FCRA) provides individuals with the right to dispute and demand correction of information about them that is held by consumer reporting agencies.

Compensation

39 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to monetary damages for wrongful acts under common law and pursuant to most statutes that provide for a private right of action. Consumers often bring class action lawsuits against organisations as a result of alleged privacy violations, such as statutory violations or other wrongful acts that affect them, such as information security breaches. In security breach cases, consumers often allege that the organisation was negligent in securing the consumers' personal information, and that such negligence led to the security breach. As a general matter, consumers would need to establish that they suffered actual damages as a direct result of the organisation's negligence in order to succeed on their claim.

In the regulatory context, the ability to obtain monetary damages or compensation depends entirely on the statute in question. Under section 5 of the Federal Trade Commission Act (FTC Act), for example, equitable relief is available first but then monetary penalties could reach $41,484 per violation for a breach of a consent order. Pursuant to the FCRA, in the event an organisation is wilfully non-compliant with the law, the Act provides for the recovery by aggrieved individuals of actual damages sustained or damages of 'not less than $100 and not more than $1,000' per violation, plus punitive damages, attorneys' fees and court costs. Negligent non-compliance may result in liability for actual damages as well as costs and attorneys' fees. Other laws, such as section 5 of the FTC Act, provide no private right of action to individuals and instead can be enforced solely by the regulator.

Enforcement

40 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

To the extent an individual obtains monetary relief as a result of illegal activity by an organisation, that relief will be obtained primarily through the judicial system. Typically, the civil penalties imposed by regulators are not paid directly to aggrieved individuals. There are, however, exceptions to this rule. For example, under the FCRA, organisations that settle claims with regulators can be asked to provide funds for consumer redress.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There is no law of general application regarding privacy and information security in the United States, and thus there are no derogations, exclusions or limitations of general application as there are in other jurisdictions. Cybersecurity Information Sharing Act (CISA) provides companies with liability protection for cybersecurity monitoring and defence practices. For example, CISA pre-empts state law and grants liability protection to companies against any cause of action in any court for the monitoring of an information system and information to the extent the monitoring is conducted for cyber-security purposes delineated under the CISA.

SUPERVISION

Judicial review

42 Can PII owners appeal against orders of the supervisory authority to the courts?

The ability of an organisation to appeal orders of a supervisory authority is highly contextual. In the Federal Trade Commission (FTC) context, an order is the result of an administrative proceeding before an FTC administrative law judge and the full FTC on review. An order issued by the FTC as a result of this process can be appealed directly to a federal court of appeals, where the FTC's order would be entitled to some deference on review.

SPECIFIC DATA PROCESSING

Internet use

43 Describe any rules on the use of 'cookies' or equivalent technology.

There have been numerous legislative efforts aimed at providing formal regulation for the use of cookies, particularly in the behavioural advertising context. To date, none of those legislative efforts has succeeded. The Federal Trade Commission (FTC) has issued a substantial amount of guidance in the area of online behavioural advertising, and industry has responded with a series of self-regulatory frameworks. Although not focused directly on cookies, there have been a number of civil actions brought by individuals and regulatory enforcement actions brought by the FTC for practices that depend on the use of cookies, but the allegations tend to focus on laws of more general application, such as surveillance laws and section 5 of the FTC Act. At the state level, California law requires website operators to disclose how the operator responds to internet browser 'do not track' signals or other mechanisms that provide consumers with the ability to exercise choice regarding the collection of personal information about an individual consumer's online activities over time and across third-party website or online services, if the operator engages in that collection. In addition, the California Consumer Privacy Act affords consumers certain rights with respect to the sale of their data, which could bear impact on the use of third-party cookies in many circumstances.

Electronic communications marketing

44 Describe any rules on marketing by email, fax or telephone.

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question. Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM. Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities. Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC. Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The National Institute of Standards and Technology has issued guidelines on security and privacy in cloud computing that are directed at federal departments and agencies. The guidelines state that the cloud computing solution should be able to meet the specific privacy and security needs of the department or agency, and departments and agencies should remain accountable for the security and privacy of any data and applications maintained in the cloud. In addition, the Department of Health and Human Services has issued guidance on Health Insurance Portability and Accountability Act of 1996 and cloud computing, clarifying that covered entities and business associates must enter into business associate agreements with cloud service providers that store or process electronic PHI before storing records containing electronic PHI in a cloud computing facility.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In 2018, the California legislature enacted the ground-breaking California Consumer Privacy Act (CCPA), which signalled a dramatic shift in the data privacy regime in the United States. With a compliance deadline in 2020, the CCPA grants consumers a number of new privacy rights. For example, a consumer has the right, subject to certain exceptions, to:

- request that an organisation provide the consumer with access to and certain details about her personal information;
- request that an organisation delete any personal information about the consumer which the organisation has collected from the consumer; and
- direct an organisation not to sell the consumer's personal information.

As such, the CCPA requires covered entities to make significant changes to their privacy programs with respect to how they collect, use and disclose personal information. Since 2018, a number of legislative proposals seeking to clarify and amend the CCPA have been introduced. Many of these proposed amendments are pending in the California legislature.

Given California's significant economic impact, and the fact that the CCPA is the most prescriptive general privacy law in the United States, the law has helped set the stage for a number of similarly-focused proposed laws currently pending in state legislatures, as well as a possible federal data privacy law.

Whether a federal law will pre-empt state laws such as the CCPA also is a topic of debate and disagreement.

HUNTON ANDREWS KURTH

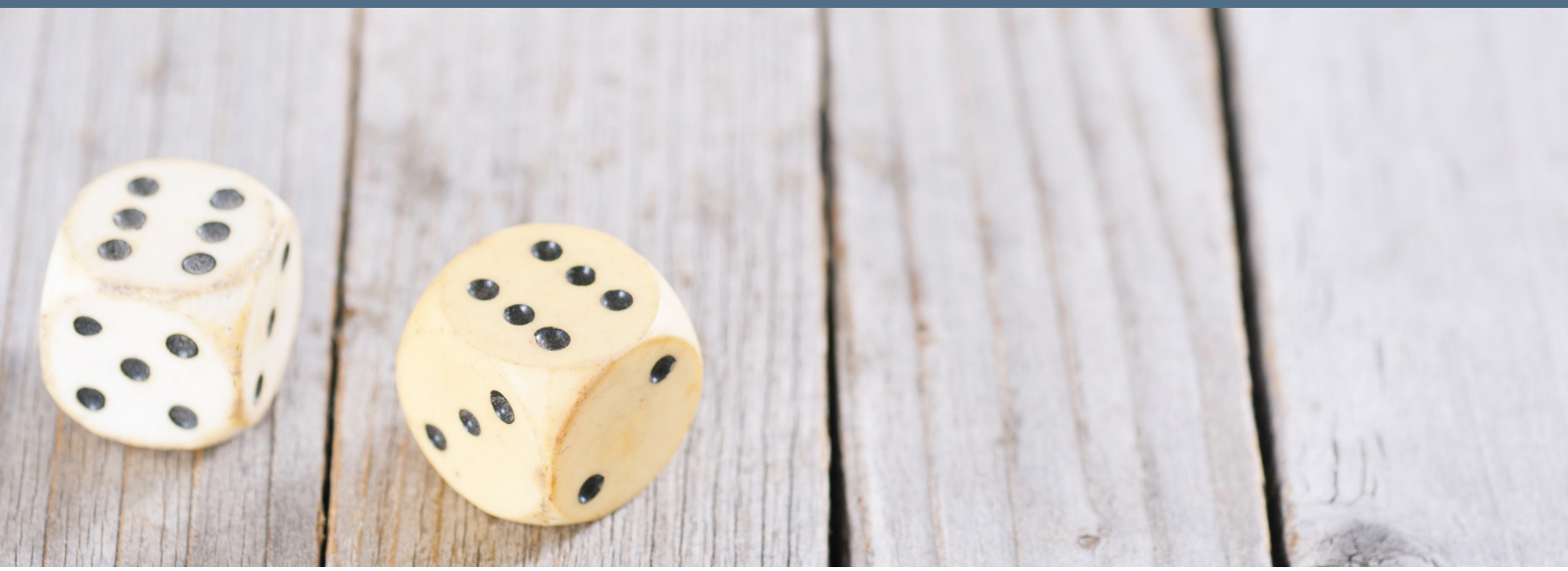
Aaron P Simpson
asimpson@huntonak.com

Lisa J Sotto
lsotto@huntonak.com

200 Park Avenue
New York
New York
10166
United States
Tel: +1 212 309 1000
www.huntonak.com

HUNTON
ANDREWS KURTH

Leaders in Handling High-Stakes Cybersecurity Events



Luck is not a strategy.

Increase your company's resilience and responsiveness to cyber attacks.

Hunton Andrews Kurth LLP's privacy and cybersecurity practice assists global organizations in managing data through every step of the information life cycle. We help businesses prepare for and respond to cybersecurity incidents all over the world. The firm is ranked as a top law firm globally for privacy and data security.

For more information, visit www.huntonprivacyblog.com.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7