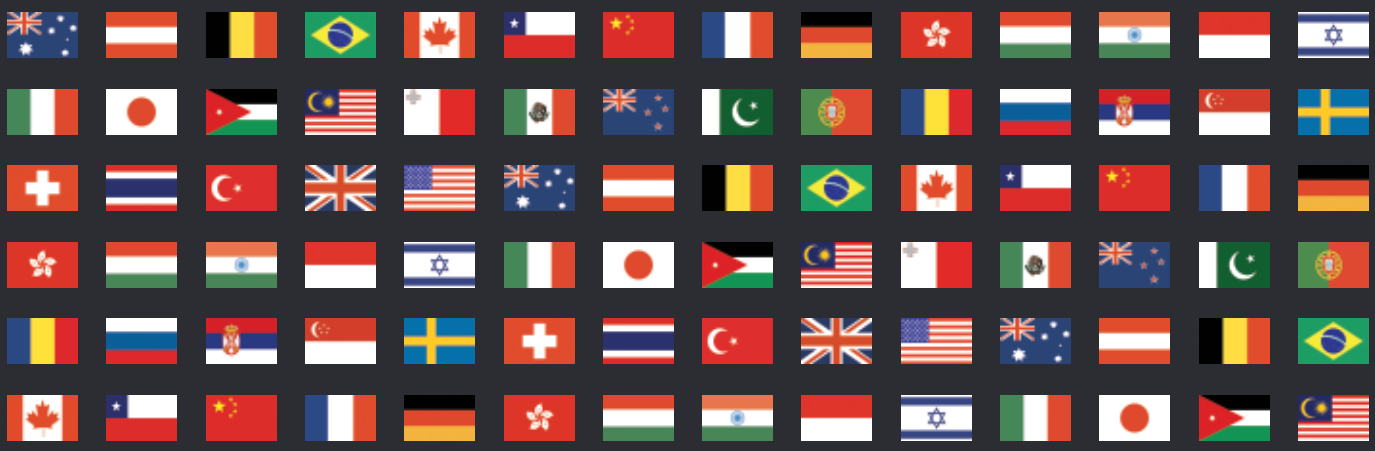
Data Protection & Privacy 2022

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

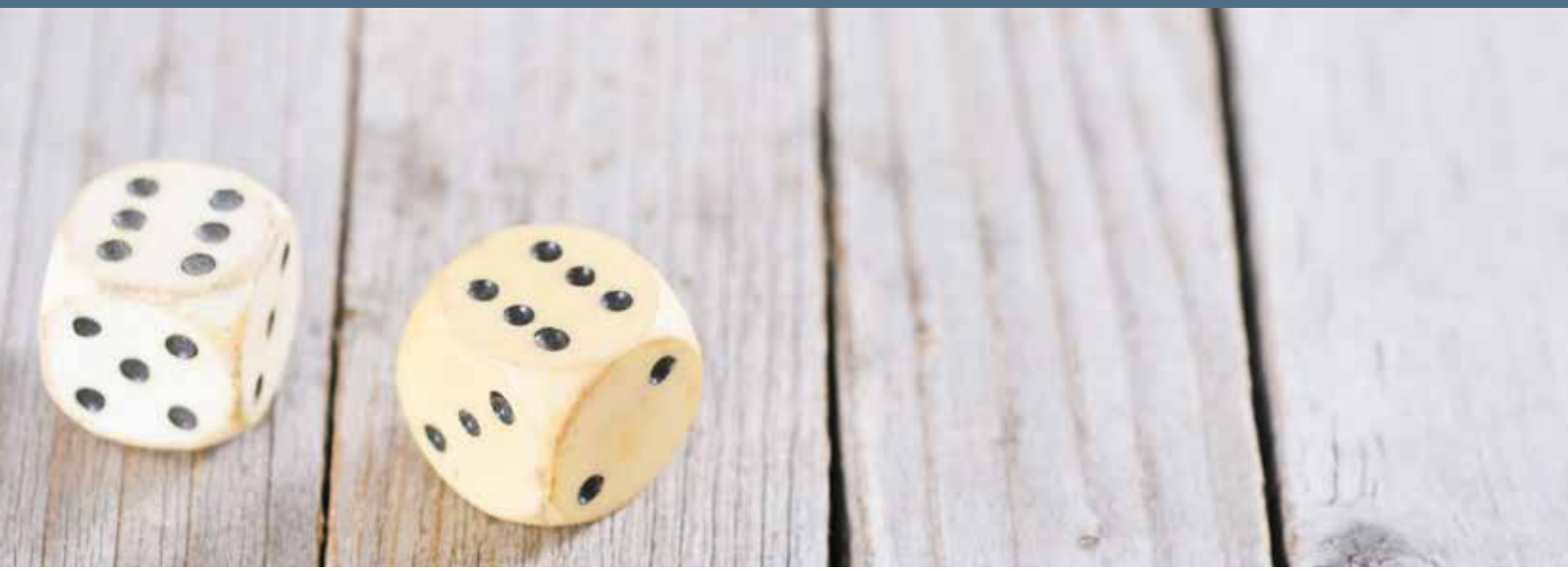


LEXOLOGY
Getting The Deal Through

HUNTON
ANDREWS KURTH

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.

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
Tenth edition
ISBN 978-1-83862-644-0

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

Data Protection & Privacy

2022

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

Lexology Getting The Deal Through is delighted to publish the tenth 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 Jordan, Pakistan and Thailand.

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.

LEXOLOGY
Getting The Deal Through

London
July 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction 5
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

EU overview 11
Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki
Hunton Andrews Kurth LLP

The Privacy Shield 14
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 20
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 28
Rainer Knyrim
Knyrim Trieb Rechtsanwälte

Belgium 37
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 49
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

Canada 57
Doug Tait and Kendall N Dyck
Thompson Dorfman Sweatman LLP

Chile 65
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 72
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

France 82
Benjamin May and Marianne Long
Aramis Law Firm

Germany 96
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Hong Kong 104
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Hungary 113
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

India 121
Arjun Sinha, Mriganki Nagpal and Siddhartha Tandon
AP & Partners

Indonesia 128
Rusmaini Lenggogeni and Charvia Tjhai
SSEK Legal Consultants

Israel 136
Adi El Rom and Hilla Shribman
Amit Pollak Matalon & Co

Italy 145
Paolo Balboni, Luca Bolognini, Davide Baldini and Antonio Landi
ICT Legal Consulting

Japan 154
Akemi Suzuki and Takeshi Hayakawa
Nagashima Ohno & Tsunematsu

Jordan 164
Ma'in Nsair, Haya Al-Erqsousi and Mariana Abu-Dayah
Nsair & Partners - Lawyers

Malaysia 170
Jillian Chia Yan Ping and Natalie Lim
SKRINE

Malta 178
Paul Gonzi and Sarah Cannataci
Fenech & Fenech Advocates

Mexico 187
Abraham Díaz and Gustavo A Alcocer
OLIVARES

New Zealand 195
Derek Roth-Biester, Megan Pearce and Victoria Wilson
Anderson Lloyd

Pakistan 202
Saifullah Khan and Saeed Hasan Khan
S.U.Khan Associates Corporate & Legal Consultants

Portugal 209
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Romania 218
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Alina Popescu
MPR Partners

Russia 226
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva and Alena Neskoromyuk
Morgan, Lewis & Bockius LLP

Serbia 235
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 242
Lim Chong Kin
Drew & Napier LLC

Sweden 257
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 265
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Taiwan 276
Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Thailand 284
John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Patchamon Purikasem
Formichella & Sritawat Attorneys at Law Co, Ltd

Turkey 291
Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Nazlı Bahar Bilhan
Turunç

United Kingdom 299
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States 309
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

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 2013, noted the rapid growth of privacy and data protection laws across the world 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 that 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

Several international instruments 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 concerning the Automatic Processing of Personal Data (Convention 108+) of the Council of Europe;
- the Organization for Economic Cooperation and Development Privacy Recommendations and Guidelines (OECD Guidelines);
- Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) of the European Union;
- 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+. Before 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, 36 countries have signed and 11 countries (Bulgaria, Croatia, Cyprus, Estonia, Finland, Lithuania, Malta, Mauritius, Poland, Serbia and Spain) 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 United States, which has accepted the Guidelines.

Convention 108+ (and its predecessor Convention 108) and the OECD Guidelines originally date from the 1980s. By the 1990s, the European Union 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 European Union, therefore, passed Directive 95/46/EC (the Data Protection Directive), which was implemented by the EU member states with a view to creating an EU-wide framework for harmonising

data protection rules. The Data Protection Directive 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 European Union. As of the date of publication, eight economies participate in the APEC CBPR system, including Australia, Canada, Japan, South Korea, Mexico, Singapore, Taiwan and the United States.

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 eight. It has been reported that several 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. Before the GDPR, each EU member state introduced legislation based on the Data Protection Directive, which made it mandatory for EU 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 continue to follow the requirements of Directive 2002/58/EC (the ePrivacy Directive) on privacy and electronic communications.

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

This was one of 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, Directive 2016/680/EU (the Police and Criminal Justice Authorities Directive). The GDPR establishes a single set of rules directly applicable throughout the European Union, intended to streamline compliance for companies doing business in the European Union. 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 European Union. The Council and the Parliament adopted the GDPR and the Police and Criminal Justice Authorities Directive 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 Authorities 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 European Union. The new rules apply to any processing of personal information conducted from outside the European Union that involves the offering of goods or services to individuals in the European Union or the monitoring of individuals in the European Union.

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 the EU member state level are not aligned and therefore businesses find themselves – once again – in a situation where they have to comply with different EU member state laws in addition to the GDPR. Further, almost all data protection authorities in the European Union have published their own guidance and recommendations on how to comply with the GDPR, regardless of the guidelines that are being adopted at the 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 the EU and member state levels 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 was 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 was intended to replace the ePrivacy Directive. The proposal was forwarded simultaneously to the European Parliament, the Council and EU 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. On 10 February 2021, after several progress reports and revised drafts of the ePrivacy Regulation, representatives of the EU member states reached an agreement on the Council of the European Union's negotiating mandate for the draft ePrivacy Regulation. The text approved by the EU member states was prepared under Portugal's presidency and will form the basis of the Council's negotiations with the European Parliament on the final terms of the ePrivacy Regulation. The Council will now begin discussions with the European Parliament to negotiate the final text. Once adopted by the Council and the European Parliament, the draft text provides for a transition period of two years, starting 20 days after the final text of the ePrivacy Regulation is published in the EU Official Journal.

In addition to revamping the legal framework for general data protection, there has been an increased focus on cybersecurity in the European Union. Since the adoption of its EU Cybersecurity Strategy in 2013, the European Commission has made laudable efforts to better protect EU citizens 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. Also, on 6 July 2016, the European Parliament adopted Directive (EU) 2016/1148 (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 EU member states had until May 2018 to transpose the NIS Directive into their national laws. On 25 June 2020, the European Commission launched a public consultation on the revision of the NIS Directive. The European Commission considers a revision to be necessary as cybersecurity capabilities in EU member states remain unequal despite progress made with the NIS Directive, and the level of protection in the European Union is insufficient. Also, the rapid digitalisation of society has expanded the threat landscape and presents new challenges requiring adaptive and innovative responses.

In 2016, the United Kingdom voted in a referendum to leave the European Union. In March 2017, the UK government formally notified the European Union of the UK's referendum decision, triggering article 50 of the EU's Lisbon Treaty. This signalled the beginning of the process of the UK leaving the European Union. The United Kingdom left the European Union on 31 January 2020 and entered a Brexit transition period that ended on 31 December 2020. Following the end of the transition period, the GDPR no longer applies directly in the United Kingdom. In its place, the UK government enacted the Data Protection, Privacy and Electronic Communications (Amendments, etc) Regulations 2019 (EU Exit), which amends the UK Data Protection Act 2018 and merges it with the requirements of the GDPR to form a data protection regime that will work in a UK context after Brexit. This new regime is known as 'the UK GDPR'.

On 24 December 2020, the European Union and the United Kingdom reached an agreement in principle on the EU–UK Trade and Cooperation Agreement (the Trade Agreement). The Trade Agreement includes a further transition period of up to six months to enable the European Commission to complete its adequacy assessment of the UK's data protection laws. While the Trade Agreement did not include an adequacy determination, both the European Union and the United Kingdom have expressed a desire to grant formal data protection adequacy status to the United Kingdom. The further transition period began on 1 January 2021 and ends either on the date on which an adequacy decision concerning the United Kingdom is adopted by the European Commission or four months after the further transition period began, which shall be extended by two months unless either the European Union or the United Kingdom objects. During the further transition period, personal data can continue to be exported from the European Union to the United Kingdom without the implementation of a data transfer mechanism, such as EU Standard Contractual Clauses. Following the expiration of a further transition period, if an adequacy decision is not made, transfers of personal data from the European Union to the United Kingdom will be prohibited unless EU data exporters take further steps to ensure adequacy for personal data. Those steps include entering into the EU Standard Contractual Clauses.

On 19 February 2021, the European Commission published a draft data protection adequacy decision relating to the United Kingdom. If the draft decision is adopted, organisations in the European Union will be able to continue to transfer personal data to organisations in the United Kingdom without restriction, and will not need to rely upon data transfer mechanisms, such as the EU Standard Contractual Clauses, to ensure an adequate level of protection. In reaching the decision, the European Commission analysed the data protection legal framework in the United Kingdom and concluded that the UK's data protection regime meets EU data protection adequacy requirements. On 14 April 2021, the European Data Protection Board (the EDPB) announced that it had adopted its Opinion on the draft UK adequacy decision issued by the European Commission. The EDPB's Opinion is non-binding but will be persuasive. Following the EDPB's Opinion, the adequacy decision will be formally adopted if it is approved by the EU member states acting through the European Council, which is considered likely. If adopted, transfers of personal data from the European Union to the United Kingdom may continue following the end of the post-Brexit transition period without restriction.

Global perspective

The United States and the European Union

Moving outside Europe, the picture is more varied. From an EU perspective, the United States is considered to have less regard for the importance of personal information protection. However, the United States has had a Privacy Act regulating government departments and agencies since 1974, and there are hundreds of privacy laws at the federal and state-level governing various types of information and data processing activities (eg, surveillance laws, biometric data laws and laws requiring online privacy policies, etc). Contrary to the EU's omnibus law approach, the United States 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. It has also adopted specific privacy rules for health-related data, the Health Insurance Portability and Accountability Act, and for financial institutions, the Gramm-Leach-Bliley Act. 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. In November 2020, California voters approved Proposition 24, a ballot referendum to amend the CCPA. Proposition 24, titled the California Privacy Rights Act of 2020 (CPRA), expands certain of the CCPA's compliance obligations and consumer rights. The CPRA will take effect on 1 January 2023. Inspired by California, numerous other states have considered or are actively considering similarly comprehensive privacy legislation. In March 2021, Virginia became the second state to enact comprehensive privacy legislation when it enacted the Consumer Data Protection Act (VCDPA). The VCDPA is similar in certain respects to both the GDPR and the CCPA, though contains key distinctions. As a result of this state legislative activity, and absent a comprehensive federal privacy and data security law, US businesses are having to contend with a patchwork of different state requirements.

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 issued guidelines and procedures for sharing information under the CISA. The Judicial Redress Act was enacted in February 2016 as a gesture to the European Union that the United States 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, then-President Trump signed an executive order aimed at strengthening the cybersecurity of federal networks and critical infrastructure.

The United States 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 European Union to the United States. This formal finding of adequacy for companies that joined and complied with the Safe Harbor was heavily criticised in the European Union 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 European Union to the United States. 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.

Following the EU–US Privacy Shield adequacy decision that was adopted in July 2016, the first joint annual review of the EU–US 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 EU–US Privacy Shield while outlining certain areas in need of improvement, including the need for ongoing monitoring of compliance with the EU–US Privacy Shield Principles by the Department of Commerce and strengthening of the privacy protections contained in the US Foreign Intelligence Surveillance Act. The EU–US 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 concerning the Foreign Intelligence Surveillance Act and highlighted several steps that should be taken to better ensure the effective functioning of the EU–US Privacy Shield (eg, 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 EU–US Privacy Shield on 16 July 2020. In Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case C 311/18) (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 United States. 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. Since the Schrems II decision, US and EU authorities have been negotiating a revised data transfer framework, with those negotiations intensifying in the spring of 2021, as indicated on 25 March 2021 joint statement by US Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders. The Biden administration has stated that establishing a successor agreement to the EU–US Privacy Shield is a top priority of the Department of Commerce.

The European Commission has recently adopted new Standard Contractual Clauses (new SCCs) in replacement of the existing controller-to-controller and controller-to-processor standard contractual clauses, adopted in 2004 and 2010 respectively. The new SCCs may be used by entities subject to the GDPR to ensure an adequate level of protection for personal data transferred to recipients located in jurisdictions not deemed by the European Union to provide an adequate level of protection for personal data transferred, including the United States. The new SCCs adopt a modular approach and include provisions that may be used for controller-controller, controller-processor, processor-processor and processor-controller data transfers. While the existing standard contractual clauses have remained a valid data transfer mechanism since the GDPR came into effect, they were drafted under the Data Protection Directive and so do not sit comfortably alongside many of the updates to the EU data protection framework made by the GDPR. The primary purpose of the new SCCs is to provide a data transfer mechanism that operates seamlessly with the legal framework of the GDPR. Also, following the Schrems II decision, the CJEU held that organisations relying on the standard contractual clauses are required to carry out a case by case assessment of whether the standard contractual clauses, in fact, provide an adequate level of protection, and requires organisations to adduce additional contractual, technical and organisational safeguards where that is not the case. While the new SCCs are unlikely to alleviate such requirements entirely, the new SCCs do impose additional obligations on data importers concerning their handling of government requests for disclosure of or access to EU personal data. At this point in time, the extent to which those provisions are likely to be considered sufficient by EU supervisory authorities remains to be seen. It also should be noted that the new SCCs have not and will not be approved for transfers of personal data by organisations located in the United Kingdom. The UK Information Commissioner's Office has indicated that it intends to publish standard contractual clauses for use by UK exporters in 2021.

Asia-Pacific

In the Asia-Pacific region, the early adopters of privacy and data protection laws – Australia, New Zealand and the Hong Kong Special Administrative Region – 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. New Zealand also amended its privacy law to enact mandatory data breach notification, effective since December 2020. China adopted the 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 concerning the Cybersecurity Law, including draft guidelines concerning the security assessment of cross-border transfers of personal information and important data. Further, 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 2021, China also issued a draft Personal Information Protection Law, marking the introduction of a comprehensive system for the protection of personal information in China; the April 2021 draft was a second version of the bill previously introduced on 21 October 2020 and was issued for public comment.

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. An additional consultation paper was introduced in January 2020 to propose certain changes to the data protection law, but as of the date of this publication, there is no indication of a timeline for amendments to the data protection law

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 European Union 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 European Union 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. In 2017, the Malaysian data protection authority launched a public consultation on the rules regarding cross-border data transfers, which included an initial whitelist of jurisdictions deemed adequate for overseas transfers, but as of the date of this publication, the final whitelist had not been approved. 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. In February 2021, Singapore enacted a mandatory data breach notification law to replace previous non-binding breach notification guidance.

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 introduced, 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 enforcement; however, the implementation deadline subsequently was extended until 1 June 2021.

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. Vietnam also enacted a Cybersecurity Law in June 2018, but there remains no single comprehensive data protection law in that jurisdiction.

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 2021, and a national data protection authority was established in 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.

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, approximately half of the 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 took effect on 1 July 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 the Cybercrimes and Cybersecurity Bill in December 2017, but the Bill was tabled in Parliament. 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 GDPR, while Morocco published a Q&A in June 2017 and held a seminar in July 2018 on the impact of the GDPR on Moroccan companies. In November 2019, Kenya's comprehensive Data Protection Act entered into force. Most recently, in early 2021, Rwanda approved a comprehensive data protection law.

The Middle East

In the Middle East, several laws 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 (DIFC) Authority of the United Arab Emirates 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. In July 2020, the DIFC enacted a replacement for the previous data protection law in that jurisdiction. The new DIFC data protection law took effect on 1 October 2020. The new data protection law was, in part, an effort to help ensure that the DIFC, a financial hub for the Middle East, Africa and South Asia, meets the standard of data protection required to receive an 'adequacy' finding from the European Commission and the United Kingdom to facilitate cross-border transfers of EU–UK personal data to the DIFC without a separate data transfer mechanism.

Conclusion

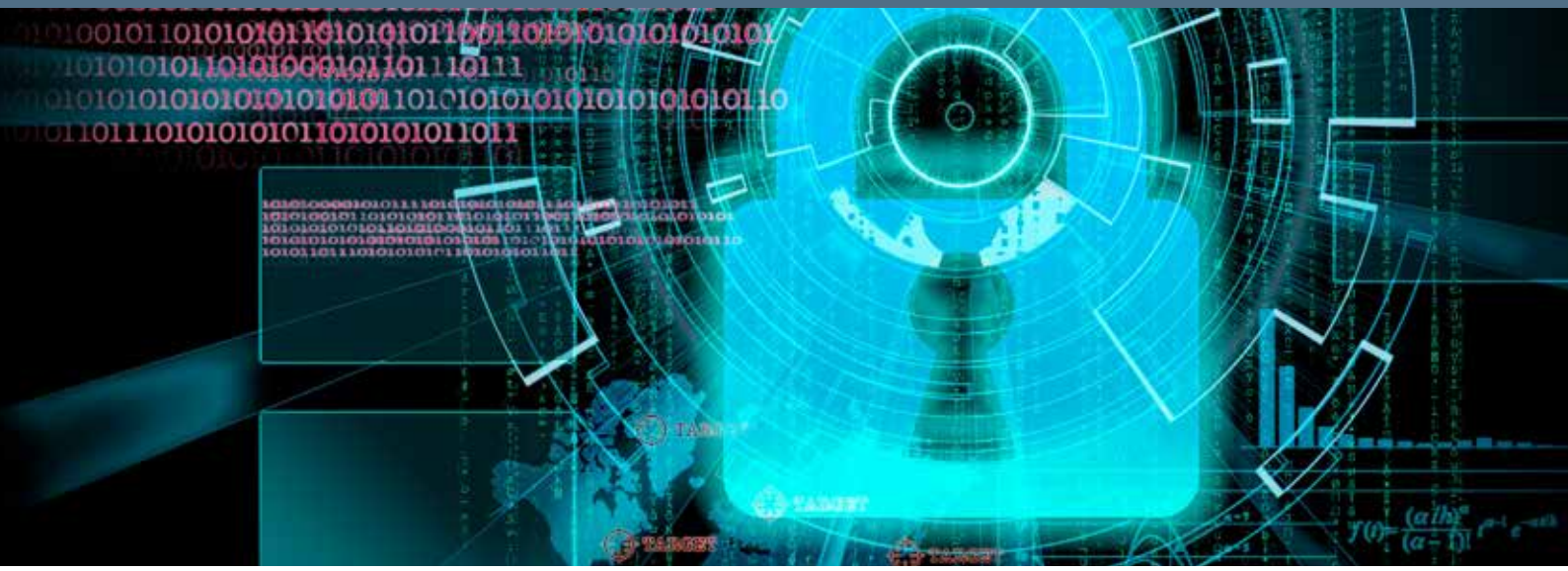
Now more than ever, global businesses face the challenge of complying with myriad laws and regulations on privacy, data protection and cybersecurity. This can make it difficult to roll out new programmes, technologies and policies with a single, harmonised approach. In some countries, restrictions on 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 to govern data protection.

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.

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.

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 978-1-83862-644-0