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

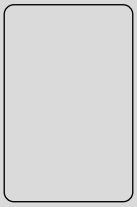
Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

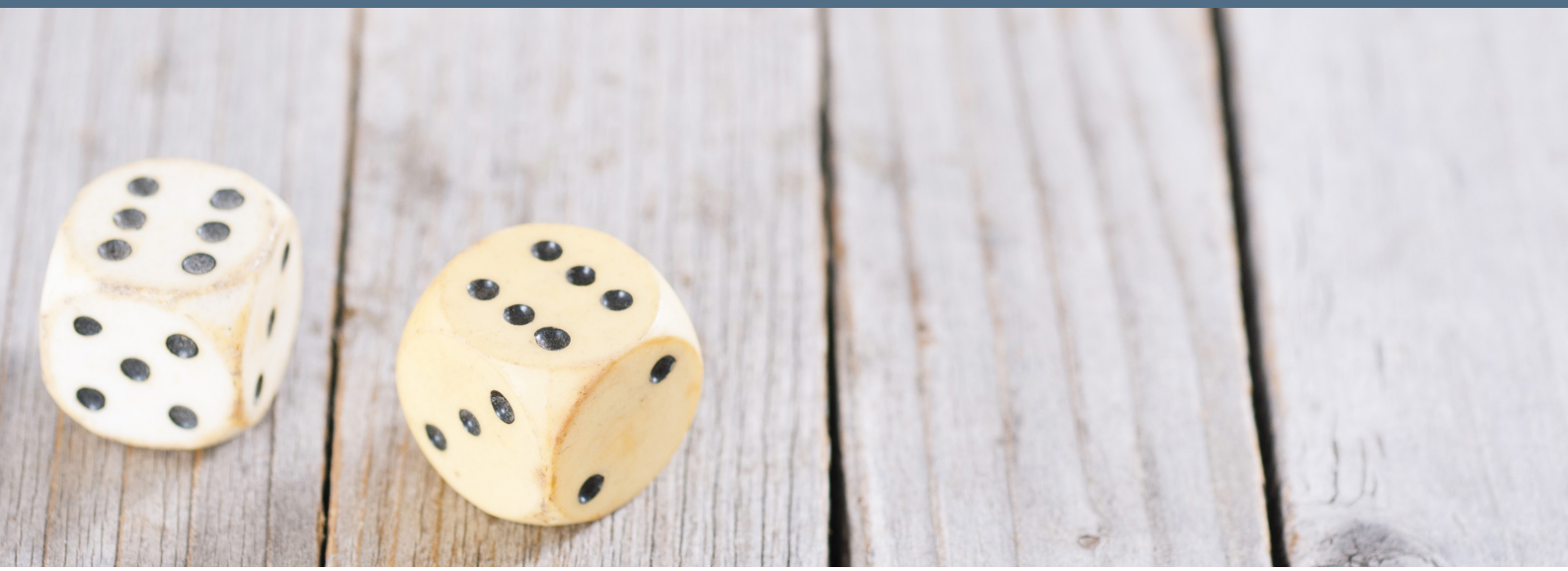
In the Middle East there are several laws that cover specific industry sectors but, apart from Israel, few countries have comprehensive data protection laws. Israel updated its data protection law in March 2017 by adding data security-related obligations, including data breach notification requirements. 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.

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