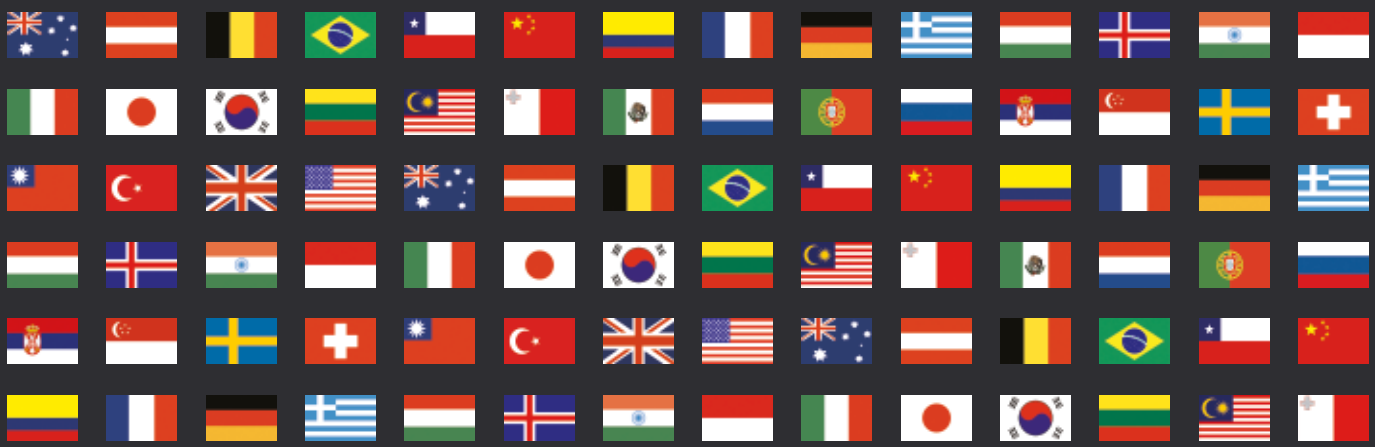
Data Protection & Privacy 2020

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 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 managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2012
Eighth edition
ISBN 978-1-83862-146-9

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

Data Protection & Privacy

2020

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

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and 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 Hungary, Iceland, Indonesia and Malaysia.

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 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

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 was expected to apply in the EEA EFTA member states (Iceland, Liechtenstein and Norway) in mid-July 2018. The GDPR replaces the EU Data Protection Directive (Directive 95/46/EC) dated 24 October 1995, and aims to establish 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 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 disagreement among DPAs with regard to possible enforcement action, the matter can be escalated to the 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. Although DPAs have adopted tools for cooperation between them, it remains to be seen how the one-stop shop mechanism will work in practice. Businesses will have to approach the DPA they consider as their lead DPA, for example, in France, 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. The GDPR imposes shared 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. Data processors are required to assist data controllers in ensuring compliance with their accountability obligations. 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 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 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. 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 introduces requirements for 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'. The right to be forgotten 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. 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. 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.

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 turnover, 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 has been 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

- codes of conduct and monitoring bodies;
- the accreditation of certification providers under article 43;
- the territorial scope of the GDPR; and
- data transfer restriction derogations under article 49.

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 introduce or maintain 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 21 June 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 (Datenschutz-Anpassungsgesetz 2018). At the time of writing, not all EU member states 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.

It is fair to say that the GDPR sets the stage for a more robust and mature data protection framework in the EU for the foreseeable future, 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 be prepared for the new challenges and at the very least be able to demonstrate that they have engaged in a GDPR compliance programme, in light of the DPA inspections that are expected to be carried out in the coming months.

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@HuntonAK.com

Claire François
cfrancois@HuntonAK.com

James Henderson
jhenderson@HuntonAK.com

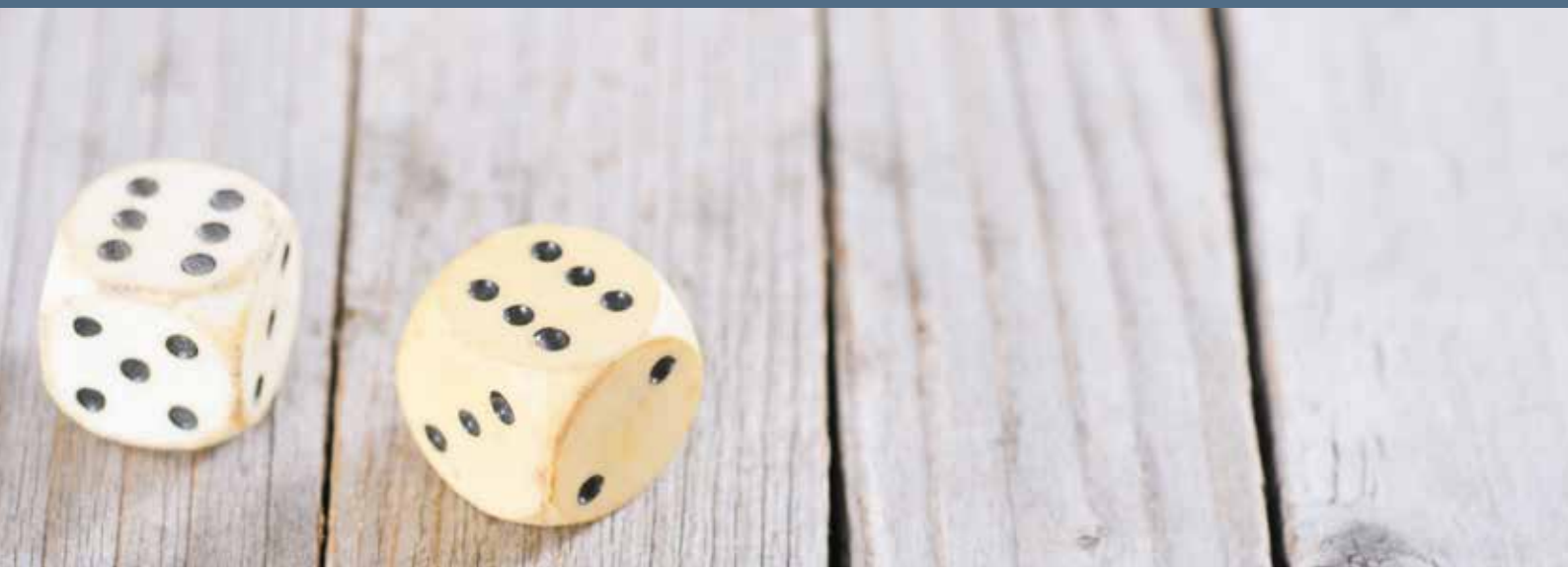
30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
Tel: +32 (0)2 643 58 00
Fax: +32 (0)2 643 58 22

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
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
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
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
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
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

ISBN 978-1-83862-146-9