# 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

# EU overview

**Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki**

Hunton Andrews Kurth LLP

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) became directly applicable in all EU member states from 25 May 2018 and in the European Free Trade Association member states of the European Economic Area (Iceland, Liechtenstein and Norway) in July 2018. The GDPR replaced EU Directive 95/46/EC (the Data Protection Directive) of 24 October 1995, and established a single set of rules throughout the European Union, 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 several guidelines on how to interpret and implement the legal framework. This provides useful guidance to businesses on how to align their data protection practices with the GDPR

**Territorial scope**

The GDPR is relevant to both EU businesses and non-EU businesses processing the personal data of individuals in the European Union. Concerning businesses established in the European Union, 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 European Union. The GDPR applies to non-EU businesses if they target individuals in the European Union by offering them products or services, or if they monitor the behaviour of individuals in the European Union.

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

**Accountability**

Under the GDPR, businesses are held accountable concerning their data processing operations and compliance obligations, and the GDPR includes a general accountability principle that requires controllers to be able to demonstrate their compliance with the GDPR's obligations. The GDPR also imposes several specific obligations on data controllers and data processors in this respect. Data controllers are required to implement and update – where necessary – appropriate technical and organisational measures to ensure that their data processing activities are carried out in compliance with the GDPR and to document these measures to be able 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 and privacy by 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 have to be conducted in cases of high-risk data processing, and certain other specified processing activities, such as those that involve the processing of sensitive data on a large scale. Data processors are required to assist data controllers in ensuring compliance with their accountability obligations, including DPIAs, the implementation of appropriate security measures, and the handling of data subject rights requests. Also, data controllers and data processors have to implement robust data security measures and keep internal records of their data processing activities. Further, 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 introduced a general data breach notification requirement applicable to all industries. All data controllers 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. Also, data controllers have to notify affected individuals if the breach is likely to result in a high risk to the individuals' rights and freedoms. Businesses must maintain data breach response plans and take other breach readiness measures to avoid fines and the negative publicity associated with data breaches. Data processors are required to notify data controllers of personal data breaches without undue delay after becoming aware of a breach but do not have an independent obligation to notify DPAs or affected individuals.

**Data processing agreements**

The GDPR imposes requirements regarding content that must 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 European Union), 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, restrictions on the use of sub-processors, and an obligation to delete or return personal data to the data controller upon the termination of the services. The EDPB and some DPAs (eg, the Danish, 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 consent, such as in employment matters. Electronic consent is acceptable, but it has to be clear, concise and not unnecessarily disruptive. In the context of a service, the provision of the service should not be made conditional on customers consenting to the processing of personal data that is not necessary for the service. Further, the GDPR requires data controllers to make additional arrangements to ensure they obtain, maintain and can demonstrate valid consent.

**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 data controller's data retention practices, how individuals can obtain a copy of the data transfer mechanisms that have been implemented, information about data recipients 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 (eg, the use of a layered privacy notice in a digital context). These transparency requirements require businesses to review their privacy notices regularly.

**Rights of individuals**

The GDPR strengthens the traditional rights of individuals, such as the rights of access, correction and erasure, and introduces additional rights. For instance, the GDPR strengthens the right of individuals to object to the processing of their personal data. Also, the GDPR enhances the right to have personal data erased by introducing a 'right to be forgotten'. The right of erasure generally 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, however it is subject to restrictions. The additional 'right to be forgotten' requires that the data controller communicates a request for the erasure of personal data to other data controllers where the data controller has made the personal data public. Further, 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 concerning automated processing based on consent or processing that is necessary for the performance of a contract. Individuals may also have a right to restrict the processing of personal data in some circumstances, such as while the accuracy of personal data is verified by the data controller. Businesses must maintain policies and procedures to give effect to the rights of individuals under the GDPR.

**Data transfers**

The GDPR maintains the general prohibition of data transfers to countries outside of the European Union that do not provide an 'adequate' level of data protection but introduces alternative tools for transferring personal data outside of the European Union, such as codes of conduct and certification mechanisms. The previous contractual options for data transfers have been expanded and made easier; regulators may also adopt standard contractual clauses for data transfers to be approved by the European Commission, and it is no longer required to obtain the DPAs' prior authorisation for transferring personal data outside of the European Union and submit copies of executed standard contractual clauses (which was previously required in some member states). Also, 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 European Union – as a valid data transfer mechanism for both data controllers and data processors. As a result of the Court of Justice of the European Union decision in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C 311/18) (*Schrems II*), the EU–US Privacy Shield Framework is no longer a valid mechanism for transfers of personal data to the United States, and organisations that rely on standard contractual clauses (and other transfer mechanisms, such as BCRs) must assess each data transfer on a case by case basis to determine whether there is an adequate level of protection for personal data transferred outside the European Union and, where necessary, implement additional technical, contractual and organisational safeguards for the transfer. Also, the European Commission has issued new draft Standard Contractual Clauses for international data transfers that were adopted on 4 June 2021.

**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. EU 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. Also, 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 and EDPB GDPR guidance**

The Article 29 Working Party (WP29), composed of representatives of DPAs, has ceased to exist and was replaced by the EDPB on 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 the 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.

Also, the EDPB has adopted guidelines under the GDPR that relate to the following:

- consent under the GDPR;
- processing of personal data through video devices;
- processing in the context of the provision of online services to data subjects;
- accreditation of certification bodies under article 43;
- territorial scope;
- derogations from the prohibition on data transfers;
- the use of location data and contact tracing tools in the context of the covid-19 pandemic;
- processing of data concerning health for scientific research in the context of the covid-19 pandemic;
- criteria of right to be forgotten in search engines;
- concepts of controller and processor in the GDPR;
- data protection by design and by default;
- European Essential Guarantees for surveillance measures;
- measures that supplement transfer tools;
- interplay of Directive (EU) 2015/2366 (Payment Services Directive 2) and the GDPR;
- (EU member state) restrictions under article 23 (national or public security, etc);
- examples regarding data breach notification;
- connected vehicles and mobility related applications;
- virtual voice assistants;
- relevant and reasoned objection under the GDPR;
- certification criteria;
- application of article 65(1)(a) of the GDPR (ie, dispute resolution);
- targeting of social media users; and
- legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions.

**EU member state complementing laws**

Although the main objective of the GDPR is to harmonise data protection law across the European Union, EU member states can and have introduced additional or more specific rules in certain areas; for example, if processing involves health data, genetic data, biometric data, employee data or national identification numbers, or if processing personal data serves archiving, scientific, historical research or statistical purposes. Also, 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 Belgian Data Protection Act and the age of 14 in the Austrian Data Protection Amendment Act 2018. At the time of writing, all EU member states other than Slovenia have adopted their new national data protection laws. This creates additional layers of complexity for businesses, which should closely monitor these developments in the relevant EU member states and assess the territorial scope of the specific national rules, where applicable.

In summary, it is fair to say that the GDPR has created a robust and mature data protection framework in the European Union, while EU member state laws complement that framework. The data protection rules affect virtually any business dealing with personal data relating to individuals in the European Union. Also, the GDPR influences data protection laws in different jurisdictions around the world.

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