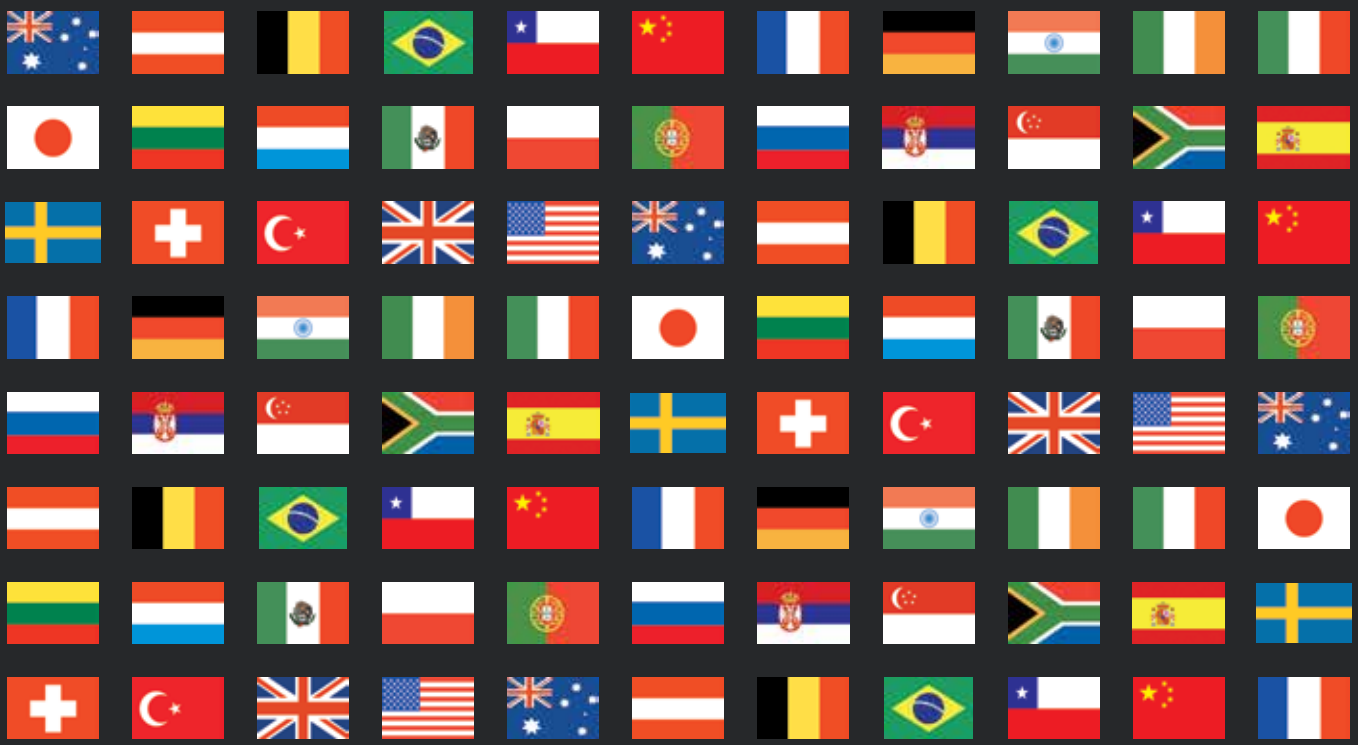
Data Protection & Privacy



2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2018

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Sixth edition
ISSN 2051-1280

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

CONTENTS

EU overview

Wim Nauwelaerts and Claire François
Hunton & Williams

The EU General Data Protection Regulation (GDPR) entered into force on 24 May 2016, and will become directly applicable in all EU member states from 25 May 2018. This two-year period is intended to allow businesses and regulators to prepare for the most significant change in EU data protection law since the enactment of the EU Data Protection Directive (Directive 95/46/EC) in 1995. The GDPR replaces the existing Directive and establishes a single set of rules throughout the EU, although EU member state data protection laws may complement these rules in certain areas. The EU data protection authorities (DPAs) gathered in the Article 29 Working Party (WP29) will publish a number of guidelines on how to interpret and implement the new legal framework. This will help businesses ensure that their existing data protection practices comply with the GDPR by May 2018.

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 EU member state DPAs, enhances cooperation between the DPAs and promotes consistency by reforming the WP29 into a separate body named the EU Data Protection Board (EDPB). 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 will now be fully affected by the GDPR.

One-stop shop
One of the most significant new concepts of 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, the GDPR 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 relevant DPA at member state level, provided that the lead DPA has been informed and agrees to the proposed course of action. Although the initial one-stop shop concept has been weakened following intense debate during the adoption of the GDPR, it remains one of the most important innovations introduced by the GDPR.

Accountability
Under the GDPR, businesses will be 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 will be 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 will be required to assist data controllers in ensuring compliance with their accountability obligations. In addition, data controllers and data processors will have to implement robust data security measures and keep internal records of their data processing activities – a system that will replace the previous requirement to register with the DPAs at member state level. Furthermore, in some cases, data controllers and data processors will be 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 will 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. Such mandatory data breach notification requirement currently exists in a handful of EU member states only. Under the GDPR, data controllers will have to notify data breaches to the DPAs without undue delay and, where feasible, within 72 hours after becoming aware of the breach. 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 will have to notify affected individuals if the breach is likely to result in high risk to the individuals' rights and freedoms. Businesses will face the challenge of developing data breach response plans and taking other breach readiness measures to avoid fines and negative publicity associated with data breaches.

Data processing agreements
The GDPR imposes minimum language that will need to be included in agreements with service providers acting as data processors. That minimum language is now much more comprehensive compared to what was required under the Directive. 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), 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 will require many businesses to review and renegotiate existing vendor and outsourcing agreements.

Consent
The GDPR explicitly confirms the currently applicable best practices regarding the conditions for obtaining individuals' consent as a legal basis for processing personal data. Consent must be based on 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 will not be valid under the GDPR. Also, consent is unlikely to be valid where there is a clear imbalance 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. 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 mechanism(s) that have been implemented, and whether personal data is used for profiling purposes. The GDPR encourages the use of standardised, machine-readable icons to provide notice about the processing, as long as such icons provide a meaningful overview of the processing in an easily visible, intelligible and clearly legible manner. In the context of services directed to children, privacy notices should be drafted in clear and plain language that children can easily understand. The new transparency requirements of the GDPR will lead 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 essentially 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 and/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 will need to review their existing practices for handling individuals' requests and consider how they will give effect to the new rights of individuals under the GDPR.

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: going forward, regulators will also be able to adopt standard contractual clauses to be approved by the European Commission. Under the GDPR, it will no longer be required to obtain the EU 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 will be able to impose administrative fines of up to €20 million or 4 per cent of a company's total worldwide annual turnover, whichever is greater. In addition, the GDPR expressly enables individuals to bring proceedings against data controllers and/or data processors, in particular to obtain compensation for damage suffered as a result of a violation of the GDPR.

The WP29 's GDPR guidance
On 3 January 2017, the WP29 adopted its second annual Action Plan, as part of its global implementation strategy of the GDPR. This complements the Action Plan for 2016, which identified the WP29's priorities for 2016 in preparing the migration to the new legal framework, namely (i) setting up the EDPB structure; (ii) preparing the one-stop shop and consistency mechanisms; (iii) issuing guidelines on four priority subjects (ie, the right to data portability; the notion of high risk and DPIAs; certification schemes and DPO designation); and (iv) communicating around the GDPR and the EDPB's role.

As part of its 2016 GDPR Action Plan, the WP29 adopted in December 2016 the first draft guidelines on the right to data portability and the designation of DPOs, as well as guidelines to help businesses identify their lead DPA in the context of the one-stop shop. On 5 April 2017, the WP29 adopted the revised and final versions of these three guidelines following a public consultation and after having examined the comments received during that public consultation. The WP29 also adopted draft guidelines on DPIAs aimed at clarifying

HUNTON& WILLIAMS

Wim Nauwelaerts **wnauwelaerts@hunton.com**
Claire François **cfrancois@hunton.com**

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 00
Fax: +32 2 643 58 22
www.hunton.com

the DPIA notion and providing criteria for member states to determine which data processing operations should be subject to a DPIA. The DPIA guidelines were open for public consultation until 23 May 2017, and the final version of these guidelines is expected to be adopted at the WP29's plenary meeting in October 2017.

In its 2017 GDPR Action Plan, the WP29 committed to finalising its work on the priorities identified in 2016, including guidelines on certification and the organisation and structure of the EDPB, as well as on the tools necessary for the cooperation between DPAs under the new framework. At the same time, the WP29 initiated its work on the new priorities established under its 2017 GDPR Action Plan, which should result in the adoption of guidelines on consent, profiling and transparency respectively, the update of already existing opinions and referentials on data transfers outside of the EU, and guidance on data breach notifications – all of this by the end of 2017.

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 impose 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 other cases than those listed in the GDPR. The new German Federal Data Protection Act, for example, requires businesses to also 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. 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. This limit is lowered to the age of 13, for example, in the new draft Polish Personal Data Protection Act that was published in March 2017. At the time of writing, most EU member states are still working on the preparation of their new national data protection laws. These new laws are expected to impose additional rules, address the procedural aspects of the new GDPR requirements at member state level, and transpose the EU Police and Criminal Justice Data Protection Directive. This will create additional layers of complexity as well as new challenges for businesses, which should closely monitor these developments in the relevant member states.

In sum, it is fair to say that the GDPR will set the stage for a more robust and mature data protection framework in the EU for the foreseeable future, while EU member state laws will complement that framework. The new rules will affect virtually any business dealing with personal data relating to individuals in the EU. Businesses should take advantage of the remaining time (until May 2018) to adapt to the new challenges and increase the level of maturity of their privacy compliance programmes.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
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 Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law