The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 2

EUROPEAN UNION OVERVIEW

William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul[1]

I OVERVIEW

In the EU, data protection is principally governed by the EU Data Protection Directive 95/46/EC[2] (Data Protection Directive), which regulates the collection and processing of personal data across all sectors of the economy.

The Data Protection Directive has been implemented in all of the 28 EU Member States through national data protection laws. The reform of EU data protection laws has been the subject of intense discussion over the past few years following the European Commission's publication in January 2012 of its proposal for an EU Data Protection Regulation,[3] which would replace the Data Protection Directive and introduce new data protection obligations for data controllers and processors, and new rights for individuals. This proposal was adopted in May 2016 as the EU's General Data Protection Regulation (Regulation)[4] and will apply in all Member States from 25 May 2018. The Regulation creates a single EU-wide law on data protection and introduces significant enforcement powers, including fines of up to 4 per cent of annual worldwide turnover or €20 million, whichever is the greater.

1 William RM Long and Alan Charles Raul are partners, Géraldine Scali is a senior associate and Francesca Blythe is an associate at Sidley Austin LLP.

2 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation).

4 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

In addition, there has also been a significant development in transatlantic data flows with the adoption, on 12 July 2016, of the EU–US Privacy Shield (Privacy Shield),[5] replacing the now invalidated US–EU Safe Harbor Framework.

Set out in this chapter is a summary of the main provisions in the Data Protection Directive and the Regulation. We then cover guidance provided by the EU's Article 29 Working Party on the topical issues of cloud computing and whistle-blowing hotlines. We conclude by considering the EU's Network and Information Security Directive (NIS Directive).

II EU DATA PROTECTION DIRECTIVE

The Data Protection Directive, as implemented into the national data protection laws of each Member State, imposes a number of obligations in relation to the processing of personal data. The Data Protection Directive also provides several rights to data subjects in relation to the processing of their personal data.

Failure to comply with the Data Protection Directive, as implemented in the national laws of EU Member States, can amount to a criminal offence, and can result in significant fines and civil claims from data subjects who have suffered as a result.

Although the Data Protection Directive sets out harmonised data protection standards and principles, the way it has been implemented by different Member States can vary significantly, with some requiring that the processing of personal data be notified to the local data protection authority (DPA).

i The scope of the Data Protection Directive

The Data Protection Directive is intended to apply to the processing of personal data wholly or partly by automatic means, and to the processing that forms part of a filing system. The Data Protection Directive is not intended to apply to the processing of personal data by an individual in the course of a purely personal or household activity.

The Data Protection Directive, as implemented through national Member State law, only applies when the processing is carried out in the context of an establishment of the controller within the jurisdiction of a Member State, or alternatively, where the controller does not have an establishment in a Member State, processes personal data through equipment located in the Member State other than for the sole purpose of transit through that Member State. There are a number of important definitions used in the Data Protection Directive, which include:[6]

a controller: any person who alone or jointly determines the purposes for which personal data is processed;

b data processor: a natural or legal person that processes personal data on behalf of the controller;

c data subject: an individual who is the subject of personal data;

5 Commission implementing decision of 12 July 2016 pursuant to Directive 95/46/EC of the Europeans Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield (Commission Implementing Decision).

6 Article 2 of the Data Protection Directive.

d establishment: a controller that carries out the effective and real exercise of activity through stable arrangements in a Member State;[7]

e filing system: any structured set of personal data that is accessible according to specific criteria, whether centralised or decentralised, such as a filing cabinet containing employee files organised according to their date of joining or their names;

f personal data: data that relate to an individual who is identified or identifiable either directly or indirectly by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In practice, this is a broad definition including anything from someone's name, address or national insurance number to information about their taste in clothes; and

g processing: any operation or set of operations performed upon personal data, such as collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This definition is so broad that it covers practically any activity in relation to personal data.

ii Obligations of controllers under the Data Protection Directive

Notification

Each Member State is obliged to set up a national DPA that controllers may be required to notify before commencing processing.[8] There are instances where some Member States can exempt controllers from this requirement. For example, if the controller has appointed a data protection officer who keeps an internal register of processing activities.[9]

Conditions for processing

Controllers may only process personal data if they have satisfied one of six conditions:

a the data subject in question has consented to the processing;

b the processing is necessary to enter into or perform a contract with the data subject;

c the processing is necessary for the pursuit of a legitimate interest of the controller or a third party to whom the personal data are to be disclosed and the rights of the data subject not overridden;

d the processing is necessary to comply with a legal obligation;

e the processing is necessary to protect the vital interests of the data subject; or

f the processing is necessary for the administration of justice or carried out in fulfilment of a public interest function.

---

7 Recital 19 of the Data Protection Directive.

8 Article 18 of the Data Protection Directive.

9 For example, in Germany, the notification requirement does not apply if the data controller has appointed a data protection officer (Section 4d(2) of the Federal Data Protection Act); or if the controller collects, processes or uses personal data for its own persons, and no more than nine employees are employed in collecting, processing or using personal data, and either the data subject has given his or her consent, or the collection, processing or use is needed to create, carry out or terminate a legal obligation or a quasi-legal obligation with the data (Section 4d(3) of the German Federal Data Protection Act).

Of these conditions, the first three will be most relevant to business.[10]

Personal data that relate to a data subject's race or ethnicity, political life, trade union membership, religious or other similar beliefs, health or sex life (sensitive personal data) can only be processed in more narrowly defined circumstances.[11] The circumstances that will often be most relevant to a business would be where the data subject has explicitly consented to the processing.

Provision of information

Certain information needs to be provided by controllers to data subjects when controllers collect personal data about them, unless the data subjects already have that information. This information includes the identity of the controller (or the controller's representative), the purposes of the processing and such further information as may be necessary to ensure that the processing is fair (e.g., the categories of personal data, the categories of recipients of the personal data, and the existence of rights of data subjects to access and correct their personal data).[12] In instances where the personal data are not collected by the controller directly from the data subject concerned, the controller is expected to notify this information at the time it collects the personal data or, where a disclosure is envisaged, at the time the personal data are first disclosed. In cases of indirect collection, it may also be possible to avoid providing the required information if to do so would be impossible or involve a disproportionate effort, or if the collection is intended for scientific or historical research or is collection that is mandated by law.

Treatment of personal data

In addition to notification and providing information to data subjects as to how their personal data will be processed, controllers must ensure that the personal data they process are adequate, relevant and not excessive for the purposes for which they were collected. In addition, controllers must keep the personal data accurate, up to date and in a form that permits identification of the data subject for no longer than is necessary.[13]

Security

The controller will be responsible for ensuring that appropriate technical and organisational measures are in place to protect the personal data. A controller must also choose a data processor providing sufficient guarantees as to the security measures applied by the data processor. A controller must have a written contract with the data processor under which the data processor agrees to only process the personal data on the instructions of the controller, and that obliges the data processor to also ensure the same level of security measures as would be expected from the controller.[14]

10 Article 7 of the Data Protection Directive.

11 Article 8 of the Data Protection Directive.

12 Article 10 of the Data Protection Directive.

13 Article 6 of the Data Protection Directive.

14 Article 17 of the Data Protection Directive.

Prohibition on transfers outside the EEA

Controllers may not transfer personal data to countries outside the European Economic Area (EEA)[15] unless the recipient country provides an adequate level of protection for the personal data.[16] The European Commission can make a finding on the adequacy of any particular non-EEA state, and Member States are expected to give effect to such findings as necessary in their national laws. So far, the European Commission has made findings of adequacy with respect to Andorra, Argentina, Australia, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. In addition, the United States previously reached agreement with the European Commission on a set of 'Safe Harbor' principles to which organisations in the United States may subscribe to be deemed 'adequate' to receive personal data from controllers in the EU.[17] However, this was in October 2015 declared invalid by the Court of Justice of the European Union (CJEU), leading to intense negotiations between US authorities and the European Commission to develop a replacement trans-Atlantic data transfer mechanism. Then on 12 July 2016, the Privacy Shield was adopted by the European Commission, with US companies being able to self-certify under the Privacy Shield from 1 August 2016.[18]

Where transfers are to be made to countries that are not deemed adequate, other exceptions may apply to permit the transfer.[19] These include where the data subject has unambiguously consented to the transfer, and where the transfer is necessary to perform or conclude a contract that the controller has with the data subject or, alternatively, with a third party if the contract is in the data subject's interests. In addition, the European Commission has approved the EU Model Contract Clauses, standard contractual clauses that may be used by controllers when transferring personal data to non-EEA countries (a model contract). There are two forms of model contract: one where both the data exporter and data importer are controllers; and another where the data exporter is a controller and the data importer is a data processor. Personal data transferred on the basis of a model contract will be presumed to be adequately protected. However, model contracts have been widely criticised as being onerous on the parties. This is because they grant third-party rights to data subjects to enforce the terms of the model contract against the data exporter and data importer, and require the parties to the model contract to give broad warranties and indemnities. The clauses of the model contracts also cannot be varied, and model contracts can become impractical where there are a large number of data transfers that need to be covered by numerous model contracts. However, the status of model contracts is currently uncertain, as we understand that the Irish Data Protection Commissioner has recently issued court proceedings to examine the validity of model contracts.

An alternative means of authorising transfers of personal data outside the EEA is the use of binding corporate rules. This approach may be suitable for multinational companies

15 The EEA consists of the 28 EU Member States together with Iceland, Liechtenstein and Norway.

16 Article 25 of the Data Protection Directive.

17 The US–EU Safe Harbor Framework was approved in 2000. Details of the Safe Harbor Agreement between the EU and the United States can be found in European Commission Decision 520/2000/EC.

18 Commission Implementing Decision.

19 Article 26 of the Data Protection Directive.

transferring personal data within the same company, or within a group of companies. Under the binding corporate rules approach, the company would adopt a group-wide data protection policy that satisfies certain criteria, and if the rules bind the whole group, then those rules could be approved by EU DPAs as providing adequate data protection for transfers of personal data throughout the group. The Article 29 Working Party, which is composed of representatives of each Member State and advises the European Commission on data protection matters, has published various documents[20] on binding corporate rules, including a model checklist for approval of binding corporate rules[21] with a table with the elements and principles to be found in binding corporate rules.[22]

iii Marketing

The EU Electronic Communications (Data Protection and Privacy) Directive 2002/58/EC (ePrivacy Directive) places requirements on Member States in relation to the use of personal data for direct marketing. Direct marketing for these purposes includes unsolicited faxes, or making unsolicited telephone calls through the use of automated calling machines or direct marketing by e-mail. In such instances, the direct marketer needs to have the prior consent of the recipient (i.e., consent on an 'opt-in' basis). However, in the case of e-mails, there are limited exceptions for e-mail marketing to existing customers where, if certain conditions[23] are satisfied, unsolicited e-mails can still be sent without prior consent. In other instances of unsolicited communications, it is left up to each Member State to decide whether

20 WP 133 – Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data adopted on 10 January 2007.
WP 154 – Working Document setting up a framework for the structure of Binding Corporate Rules adopted on 24 June 2008.
WP 155 – Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules adopted on 24 June 2008 and last revised on 8 April 2009.
WP 195 – Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules adopted on 6 June 2012.
WP 195a – Recommendation 1/2012 on the standard application form for approval of Binding Corporate Rules for the transfer of personal data for processing activities adopted on 17 September 2012.
WP 204 – Explanatory document on the Processor Binding Corporate Rules last adopted on 22 May 2015.

21 WP 108 – Working Document establishing a model checklist application for approval of binding corporate rules adopted on 14 April 2005.

22 WP 153 – Working Document setting up a table with the elements and principles to be found in binding corporate rules adopted on 24 June 2008.

23 Unsolicited e-mails may be sent without prior consent to existing customers if the contact details of the customer have been obtained in the context of a sale of a product or a service and the unsolicited e-mail is for similar products or services; and if the customer has been given an opportunity to object, free of charge in an easy manner, to such use of his or her electronic contact details when they are collected and on the occasion of each message in the event the customer has not initially refused such use – Article 13 (2) of the ePrivacy Directive.

such communications will require the recipient's prior consent or, alternatively can be sent without prior consent unless recipients have indicated that they do not wish to receive such communications (i.e., consent on an 'opt-out' basis).

The ePrivacy Directive imposes requirements on providers of publicly available electronic communication services to put in place appropriate security measures and to notify certain security breaches in relation to personal data. The ePrivacy Directive was also amended in 2009[24] to require that website operators obtain the informed consent of users to collect personal data of users through website 'cookies' or similar technologies used for storing information. There are two exemptions to the requirement to obtain consent before using cookies: when the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; and when the cookie is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[25]

The Article 29 Working Party has published an opinion on the cookie consent exemption[26] that provides an explanation on which cookies require the consent of website users (e.g., social plug-in tracking cookies, third-party advertising cookies used for behavioural advertising, analytics) and those that fall within the scope of the exemption (e.g., authentication cookies, multimedia player session cookies and cookies used to detect repeated failed login attempts). Guidance on how to obtain consent has been published at a national level by various data protection authorities.[27]

In July 2016, following the adoption of the Regulation, the Article 29 Working Party issued an opinion on a revision of the rules contained in the ePrivacy Directive.[28] While the Regulation does provide some rules relating to the subject matter of the ePrivacy Directive, the Article 29 Working Party is of the opinion that the ePrivacy Directive should be expanded to:

a cover all types of electronic communications while at the same time remaining technologically neutral;

b prohibit unlawful tracking and monitoring without freely given consent whether by cookies, device-fingerprinting or other technological means;

c allow users to use end-to-end encryption (without 'backdoors');

d extend the scope of rules on geolocation and traffic data to all parties; and

e maintain protection of confidentiality, but take into account new electronic communication services where this might be breached.

iv Rights of data subjects under the Data Protection Directive

Data subjects have a right to obtain access to personal data held about them, and also to be able to ask for the personal data to be corrected where the personal data is inaccurate.[29]

24 Directive 2009/56/EC.

25 Article 5(3) of the ePrivacy Directive.

26 WP 194 – Opinion 04/2012 on Cookie Consent Exemption.

27 For example: UK Information Commissioner's Office 'Guidance on the rules on use of cookies and similar technologies'; and the French Commission National de l'informatique et des libertés.

28 Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/53/EC).

29 Article 12 of the Data Protection Directive.

Data subjects also have rights to object to certain types of processing where there are compelling legitimate grounds;[30] for example, where the processing would cause the data subject unwarranted harm. Data subjects may also object to direct marketing and to decisions that significantly affect them being made solely on the basis of automated processing.

In May 2014, the CJEU issued a judgment against Google Inc and Google Spain SL in which it ruled that in certain circumstances, search engines are obliged to remove links displayed following a search made on the basis of a person's name, where the data is incomplete or inaccurate, even if the publication itself on those web pages is lawful. This is based on existing rights under the EU Data Protection Directive to rectification, erasure or blocking of personal data where the individual objects to the processing of such data for compelling legitimate grounds, where the data is inadequate, irrelevant or inaccurate, or excessive in relation to the purposes of the processing, and where the impact on an individual's privacy is greater than the public's right to find the data. As at May 2015, Google had received over 253,000 removal requests and had removed approximately 380,000 links from search results.

III EU DATA PROTECTION REGULATION

The Regulation was published by the European Commission in January 2012, and has been described as the most lobbied piece of European legislation in history, receiving over 4,000 amendments in opinions from committees in the European Parliament as well as from numerous industries. In March 2014, the European Parliament's Civil Liberties Committee after several delays finally voted on the European Commission's proposed EU Data Protection Regulation and adopted all amendments. Over a year later, in June 2015, the Council of Ministers (which represents EU Member States) published its compromise proposal for the Regulation. This in turn, triggered the commencement of the 'trilogue' process – the final stage of negotiations between the three EU institutions. In May 2016, after almost four years of intense negotiations, the Regulation was adopted by the European Parliament at second reading. The Regulation will apply in Member States from May 2018.

The Regulation as adopted will have a significant impact on many governments, businesses and individuals both in and outside the EU. The main elements of the Regulation are summarised below.

i Enforcement

The Regulation provides for substantial penalties in the form of administrative fines from DPAs. This is an area that underwent much negotiation and change throughout the various stages of negotiation of the Regulation.

As adopted, the Regulation provides a two-tier structure for fines. Functional, operational or administrative infringements of the Regulation will result in fines of up to €10 million or 2 per cent of annual turnover, whichever is the greater. Whereas, intentional or negligent infringements, or infringements that involve multiple provisions of the Regulation, will be subject to higher fines of up to €20 million or 4 per cent of annual turnover, whichever is the greater. In addition, the Regulation grants data subjects the right to claim damages for

30 Article 14 of the Data Protection Directive.

non-financial losses, such as distress. These extensive penalties represent a significant change in the field of data protection that should ensure that businesses and governments take data protection compliance seriously.[31]

ii Scope of the Regulation

The Regulation will apply to the processing of personal data in the context of the activities of a data controller or a processor in the EU and to a controller or processor not established in the EU where the processing activities are related to the offering of goods or services to EU citizens, or the monitoring of such individuals. This means that many non-EU companies that have EU customers will now need to comply with the Regulation.[32]

iii One-stop shop

The Regulation proposes a new regulatory 'one-stop shop' for data controllers that operate in several EU countries. The DPA where the controller is established will be the lead DPA, which must consult with other DPAs before taking action.[33] In the case of a dispute between DPAs, action can be decided upon by the European Data Protection Board. The Regulation also promotes cooperation among DPAs by requiring the lead DPA to submit a draft decision on a case to the concerned DPAs, which they will have to reach a consensus on prior to finalising any decision.[34]

iv Profiling

Significantly for online companies, under the Regulation, every individual will now have a general right to object to profiling. In addition, the Regulation imposes a new requirement to inform individuals about the right to object to profiling in a highly visible manner. Profiling that significantly affects the interests of an individual can only be carried out under limited circumstances, such as with the individual's consent, and should not be automated but involve human assessment. These provisions will have a major impact on how online companies market their products and services, and on how many organisations engage in, for example, big data analytics. Businesses should review their current profiling activities and determine whether these should be modified to ensure compliance with the Regulation.[35]

v Consent

Under the Regulation, consent must be informed and freely given, which means that a data subject must have a genuine choice as to whether to consent or not. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations.[36] Unlike under the Directive, controllers and processors cannot rely on implied or opt-out consent, and consent should be given by a clear, affirmative act, which

31 Article 83 of the Regulation.
32 Article 3 of the Regulation.
33 Article 56 of the Regulation.
34 Article 60 of the Regulation.
35 Article 22 of the Regulation.
36 Recital 43 of the Regulation.

may include, for example, ticking a box on a website.[37] In addition, it should also be as easy to withdraw consent as it is to give it, with consent being invalid where given for unspecified data processing.[38] Processing data on children under the age of 16 also requires the consent of the parent or legal guardian. Member States are entitled to set a lower age provided it is not below the age of 13.[39] Companies also cannot make the execution of a contract or a provision of a service conditional upon the receipt of consent from users to process their data.

vi Standardised information policies

The Regulation requires that data subjects be provided with extensive information relating to the processing of their personal data, including being informed about how their personal data will be processed and their rights of access to data, rectification and erasure of data and of the right to object to profiling as well as to lodge a complaint with a DPA and to bring legal proceedings.[40] In addition, the Regulation empowers the European Commission to adopt delegated acts for the purpose of providing certain information as standardised icons, as well as the procedures for providing such icons.[41]

vii Right of erasure

The 'right of erasure' (formerly the 'right to be forgotten') gives individuals a right to have their personal data erased where the data are no longer necessary or where they withdraw consent, although a limited number of exemptions also apply, such as where data are required for scientific research or for compliance with a legal obligation of EU law.[42]

viii Accountability

Controllers will be required to adopt all reasonable steps to implement compliance procedures and policies that respect the choices of individuals, which should be reviewed regularly. Importantly, controllers will need to implement privacy by design and default throughout the life cycle of processing from collection of the data to their deletion.[43] In addition, businesses will need to keep detailed documentation of the data being processed, and carry out a privacy impact assessment where the processing uses new technologies and is likely to result in a high risk for individuals, such as profiling or processing sensitive data (e.g., health data) on a large scale. This assessment also has to be reviewed regularly, and should be carried out for each new processing system or at least when there is a change in the risk represented by the processing operations.[44]

37 Recital 32 of the Regulation.
38 Article 7 of the Regulation.
39 Article 8 of the Regulation.
40 Article 12 of the Regulation.
41 Article 12 (8) of the Regulation.
42 Article 17 of the Regulation.
43 Article 25 of the Regulation.
44 Article 35 of the Regulation.

ix Data protection officers

The Regulation introduces the requirement for controllers and processors to appoint a data protection officer where the processing is carried out by a public authority; the core activities require regular and systematic monitoring of data subjects on a large scale; or the core activities consist of processing sensitive personal data on a large scale.[45]

Where required to appoint a data protection officer, the Regulation states that a group of companies can appoint a single data protection officer provided that he or she is easily accessible from each group company. In addition, there is no requirement to appoint an employee: a third party can be appointed instead. Although the Regulation does not set specific requirements in terms of the level of qualification required, the data protection officer must have expert knowledge of data protection law and practices, and be able to fulfil a prescribed list of tasks. These tasks must be carried out independently, and the data protection officer must report to the highest level of management.

x Security and security breaches

The controller and the processor will need to implement appropriate technical and organisational security measures to ensure a level of security appropriate to the risk. The Regulation also requires that security policies contain a number of elements to ensure appropriate security measures are in place, including, for example, a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.[46] In addition, security breaches will need to be notified to DPAs without undue delay and, where feasible, within 72 hours after becoming aware of the breach. Affected individuals will also need to be notified without undue delay where high risk is reported unless measures are taken to minimise the risk, such as data being encrypted.[47]

xi International data transfers

In addition to binding corporate rules and other data transfer solutions, new methods allowing for international data transfers of personal data from the EU include the use of approved codes of conduct or certification mechanisms. The Regulation also permits such international transfers where they are necessary for the 'legitimate interests' of the controller, providing such transfers are not large scale or frequent, the controller has adduced appropriate safeguards and the interests of the affected individuals are not overridden. This form of transfer is only to be used as a last resort, and organisations must inform the DPA and data subjects of its reliance on this mechanism.[48]

The Regulation also provides a mechanism that restricts Member States from enforcing a judgment issued by non-EU courts or authorities, unless the request is based on an international transfer agreement between that third country and the EU Member State.

45 Article 37 of the Regulation.

46 Article 32 of the Regulation.

47 Article 33 of the Regulation.

48 Articles 44–48 of the Regulation.

xii Health data

The Regulation also contains important provisions relating to the use of health data, including the processing of personal data for scientific research that, according to the Regulation, should be considered a compatible form of processing. This provision is important, as it may assist in allowing growth in scientific research for secondary research purposes where existing laws did not.[49]

IV CLOUD COMPUTING

In its guidance on cloud computing adopted on 1 July 2012,[50] the EU's Article 29 Working Party states that the majority of data protection risks can be divided into two main categories: lack of control over the data; and insufficient information regarding the processing operation itself. The lawfulness of the processing of personal data in the cloud depends on adherence to the principles of the EU Data Protection Directive, which are considered in the Article 29 Working Party Opinion, and some of which are summarised below.

i Instructions of the data controller

To comply with the requirements of the EU Data Protection Directive, the Article 29 Working Party Opinion provides that the extent of the instructions should be detailed in the relevant cloud computing agreement (agreement) along with service levels and financial penalties on the provider for non-compliance.

ii Purpose specification and limitation requirement[51]

Under Article 6(b) of the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. To address this requirement, the agreement between the cloud provider and the client should include technical and organisational measures to mitigate this risk, and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or subcontractors.

iii Security[52]

Under the Data Protection Directive, a data controller must have in place adequate organisational and technical security measures to protect personal data and should be able to demonstrate accountability. The Article 29 Working Party Opinion comments on this point, reiterating that it is of great importance that concrete technical and organisational measures are specified in the cloud agreement, such as availability, confidentiality, integrity, isolation and portability. As a consequence, the agreement with the cloud provider should contain a provision to ensure that the cloud provider and its subcontractors comply with the security measures imposed by the client. It should also contain a section regarding the assessment of

49 Article 9 of the Regulation.

50 WP 196 – Opinion 5/2012 on Cloud Computing.

51 Article 6(b) of the Data Protection Directive.

52 Article 17(2) of the Data Protection Directive.

the security measures of the cloud provider. The agreement should also contain an obligation for the cloud provider to inform the client of any security event. The client should also be able to assess the security measures put in place by the cloud provider.

iv Subcontractors

The Article 29 Working Party Opinion indicates that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard, with the controller retaining at all times the possibility to object to such changes or to terminate the agreement. There should also be a clear obligation on the cloud provider to name all the subcontractors commissioned, as well as the location of all data centres where the client's data can be hosted. It must also be guaranteed that both the cloud provider and all the subcontractors shall act only on instructions from the client. The agreement should also set out the obligation on the part of the processor to deal with international transfers, for example by signing contracts with sub-processors, based on the EU Model Contract Clauses.

v Erasure of data[53]

The Article 29 Working Party Opinion states that specifications on the conditions for returning the personal data or destroying the data once the service is concluded should be contained in the agreement. It also states that data processors must ensure that personal data are erased securely at the request of the client.

vi Data subject rights[54]

According to the Article 29 Working Party Opinion, the agreement should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subject's rights to access, correct or delete their data, and to ensure that the same holds true for the relation to any subcontractor.

vii International transfers[55]

As discussed above, under Articles 25 and 26 of the Data Protection Directive, personal data can only be transferred to countries located outside the EEA if the country provides an adequate level of protection.

viii Confidentiality

The Article 29 Working Party Opinion recommends that an agreement with the cloud provider should contain confidentiality wording that is binding both upon the cloud provider and any of its employees who may be able to access the data.

53 Article 6 (e) of Data Protection Directive.

54 Article 12 and 14 of the Data Protection Directive.

55 Article 25 and 26 of the Data Protection Directive.

ix Request for disclosure of personal data by a law enforcement authority

Under the Article 29 Working Party Opinion, the client should be notified about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as under a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

x Changes concerning the cloud services

The Article 29 Working Party recommends that the agreement with the cloud provider should contain a provision stating that the cloud provider must inform the client about relevant changes concerning the respective cloud service, such as the implementation of additional functions.

V WHISTLE-BLOWING HOTLINES

The Article 29 Working Party published an Opinion in 2006 on the application of the EU data protection rules to whistle-blowing hotlines[56] providing various recommendations, which are summarised below.

i Legitimacy of whistle-blowing schemes

Under the Data Protection Directive, personal data must be processed fairly and lawfully. For a whistle-blowing scheme, this means that the processing of personal data must be on the basis of at least one of certain grounds, the most relevant of which include where:

a the processing is necessary for compliance with a legal obligation to which the data controller is subject, which could arguably include a company's obligation to comply with the provisions of the US Sarbanes-Oxley Act (SOX). However, the Article 29 Working Party concluded that an obligation imposed by a foreign statute, such as SOX, does not qualify as a legal obligation that would legitimise the data processing in the EU; or

b the processing is necessary for the purposes of the legitimate interests pursued by the data controller, or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or the fundamental rights and freedoms of the data subject. The Article 29 Working Party acknowledged that whistle-blowing schemes adopted to ensure the stability of financial markets, and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting as well as the fight against bribery, banking and financial crime, or insider trading, might be seen as serving a legitimate interest of a company that would justify the processing of personal data by means of such schemes.

56 WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

ii Limiting the number of persons eligible to use the hotline

Applying the proportionality principle, the Article 29 Working Party recommends that the company responsible for the whistle-blowing reporting programme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct and the number of persons who might be incriminated. However, the recommendations acknowledged that in both cases the categories of personnel involved may still sometimes include all employees in the fields of accounting, auditing and financial services.

iii Promotion of identified reports

The Article 29 Working Party pointed out that, although in many cases anonymous reporting is a desirable option, where possible, whistle-blowing schemes should be designed in such a way that they do not encourage anonymous reporting. Rather, the helpline should obtain the contact details of reports, and maintain the confidentiality of that information within the company, for those who have a specific need to know the relevant information. The Article 29 Working Party also suggested that only reports that included identifiable information from the whistle-blower would be considered a 'fairly' collected report.

iv Proportionality and accuracy of data collected

Companies should clearly define the type of information to be disclosed through the system by limiting the information to accounting, internal accounting control or auditing, or banking and financial crime and anti-bribery. The personal data should be limited to data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

v Compliance with data-retention periods

According to the Article 29 Working Party, personal data processed by a whistle-blowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report. Such periods would be different when legal proceedings or disciplinary measures are initiated. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Personal data found to be unsubstantiated should be deleted without delay.

vi Provision of clear and complete information about the whistle-blowing programme

Companies as data controllers must provide information to employees about the existence, purpose and operation of the whistle-blowing programme, the recipients of the reports, and the right of access, rectification and erasure for reported persons. Users should also be informed that the identity of the whistle-blower shall be kept confidential, that abuse of the system may result in action against the perpetrator of that abuse, and that they will not face any sanctions if they use the system in good faith.

vii Rights of the incriminated person

The Article 29 Working Party noted that it was essential to balance the rights of the incriminated person and of the whistle-blower, and the company's legitimate investigative needs. In accordance with the Data Protection Directive, an accused person should be

informed by the person in charge of the ethics reporting programme as soon as practicably possible after the ethics report implicating them is received. The implicated employee should be informed about:

a the entity responsible for the ethics reporting programme;
b the acts of which he or she is accused;
c the departments or services that might receive the report within the company or in other entities or companies of the corporate group; and
d how to exercise his or her rights of access and rectification.

Where there is a substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather evidence, then notification to the incriminated person may be delayed as long as such risk exists.

The whistle-blowing scheme also needs to ensure compliance with the individual's right, under the Data Protection Directive, of access to personal data on them and their right to rectify incorrect, incomplete or outdated data. However, the exercise of these rights may be restricted to protect the rights of others involved in the scheme, and under no circumstances can the accused person obtain information about the identity of the whistle-blower, except where the whistle-blower maliciously makes a false statement.

viii Security

The company responsible for the whistle-blowing scheme must take all reasonable technical and organisational precautions to preserve the security of the data, and to protect against accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. Where the whistle-blowing scheme is run by an external service provider, the EU data controller needs to have in place a data processing agreement, and must take all appropriate measures to guarantee the security of the information processed throughout the whole process and commit themselves to complying with the data protection principles.

ix Management of whistle-blowing hotlines

A whistle-blowing scheme needs to carefully consider how reports are to be collected and handled with a specific organisation set up to handle the whistle-blower's reports and lead the investigation. This organisation must be composed of specifically trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations. The whistle-blowing system should be strictly separated from other departments of the company, such as human resources.

x Data transfers from the EEA

The Working Party believes that groups should deal with reports locally in one EEA state rather than automatically share all the information with other group companies. However, data may be communicated within the group if such communication is necessary for the investigation, depending on the nature or seriousness of the reported misconduct or results from how the group is set up. Such communication will be considered necessary, for example, if the report incriminates another legal entity within the group involving a high-level member of management of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient entity, which provides equivalent guarantees as regards management of the whistle-blowing reports as the EU organisation.

VI E-DISCOVERY

The Article 29 Working Party has published a working document providing guidance to data controllers in dealing with requests to transfer personal data to other jurisdictions outside the EEA for use in civil litigation[57] to help them to reconcile the demands of a litigation process in a foreign jurisdiction with the data protection obligations of the Data Protection Directive.

The main suggestions and guidelines include the following:

a Possible legal bases for processing personal data as part of a pretrial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the Article 29 Working Party states that an obligation imposed by a foreign statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. A third possible basis is a legitimate interest pursued by the data controller or by the third party to whom the data are disclosed where the legitimate interests are not overridden by the fundamental rights and freedoms of the data subjects. This involves a balance-of-interest test taking into account issues of proportionality, the relevance of the personal data to litigation and the consequences for the data subject.

b Restricting the disclosure of data if possible to anonymised or redacted data as an initial step and after culling the irrelevant data, disclosing a limited set of personal data as a second step.

c Notifying individuals in advance of the possible use of their data for litigation purposes and, where the personal data is actually processed for litigation, notifying the data subject of the identity of the recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

d Where the non-EEA country to which the data will be sent does not provide an adequate level of data protection, and where the transfer is likely to be a single transfer of all relevant information, then there would be a possible ground that the transfer is necessary for the establishment, exercise or defence of a legal claim. Where a significant amount of data is to be transferred, the Article 29 Working Party previously suggested the use of binding corporate rules or the Safe Harbor regime. However, Safe Harbor was recently found to be invalid by the CJEU. It also recognises that compliance with a request made under the Hague Convention would provide a formal basis for the transfer of the data.

VII EU CYBERSECURITY STRATEGY

In March 2014, the European Parliament adopted a proposal for the NIS Directive,[58] which was proposed by the European Commission in 2013. The NIS Directive is part of

57 WP 158 – Working Document 1/2009 on pretrial discovery for cross-border civil litigation adopted on 11 February 2009.

58 Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013.

the European Union's Cybersecurity Strategy aimed at tackling network and information security incidents and risks across the EU, and was adopted on 6 June 2016 by the European Parliament at second reading.[59]

The main elements of the NIS Directive include:

a new requirements for 'operators of essential service' and 'digital service providers';
b a new national strategy;
c designation of a national competent authority; and
d designation of computer security incident response teams (CSIRTs) and a cooperation network.

i New national strategy

The NIS Directive requires Member States to adopt a national strategy setting out concrete policy and regulatory measures to maintain a high level of network and information security.[60] This includes having research and development plans in place or a risk assessment plan to identify risks, designating a national competent authority that will be responsible for monitoring compliance with the NIS Directive and receiving any information security incident notifications,[61] and setting up of at least one CSIRT that is responsible for handling risks and incidents. [62]

ii Cooperation network

The competent authorities in EU Member States, the European Commission and ENISA, will form a cooperation network to coordinate against risks and incidents affecting network and information systems.[63] The cooperation network will exchange information between authorities and also provide early warnings on information security risks and incidents, and agree on a coordinated response in accordance with an EU–NIS cyber-cooperation plan.

iii Security requirements

A key element of the NIS Directive is that Member States must ensure public bodies and certain market operators[64] take appropriate technical and organisational measures to manage

59 Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

60 Article 7 of the NIS Directive.

61 Article 8 of the NIS Directive.

62 Article 9 of the NIS Directive.

63 Article 11 of the NIS Directive.

64 Operators of essential services are listed in Annex II of the NIS Directive and include operators in energy and transport, financial market infrastructures, banking, operators in the production and supply of water, the health sector and digital infrastructure. Digital service providers (e.g., e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores) are listed in Annex III. The requirements for digital service providers are less onerous than those imposed on operators of essential services; however, they are still required to report security incidents that have a significant impact on the service they offer in the EU.

the security risks to networks and information systems, and to guarantee a level of security appropriate to the risks.[65] The measures should prevent and minimise the impact of security incidents affecting the core services they provide. Public bodies and market operators must also notify the competent authority of incidents having a significant impact on the continuity of the core services they provide, and the competent authority may decide to inform the public of the incident. The significance of the disruptive incident should take into account:

a the number of users affected;
b the dependency of other key market operators on the service provided by the entity;
c the duration of the incident;
d the geographic spread of the area affected by the incident;
e the market share of the entity; and
f the importance of the entity for maintaining a sufficient level of service, taking into account the availability of alternative means for the provisions of that service.

Member States have until May 2018 to implement the NIS Directive into their national laws.

VIII OUTLOOK

2016 has seen a number of key developments in the European data protection world. Firstly, the Regulation was adopted in May 2016 and will apply in Member States from 25 May 2018. As the Regulation will apply extra-territorially to businesses operating outside the EU, Member States will also need to review the provisions to assess whether they fall within the scope of the Regulation, and if so, will need to make the necessary policy and procedural changes to ensure compliance. The same will apply to data processors, who are now subject to direct regulation pursuant to the Regulation.

In addition, following the invalidation of the Safe Harbor Framework, the Privacy Shield was adopted on 12 July 2016, and US companies have been able to self-certify under it since 1 August 2016. While adoption of the Privacy Shield by the European Commission does provide a degree of certainty in finding a legitimate solution for transferring data from the EU to the US, there is a substantial likelihood that the Privacy Shield will face challenges by EU DPAs and activists, but the hope is that the protections and increased level of security by US and EU regulators involved with the development of the Privacy Shield will secure its long-term future.

Other mechanisms of transfer, including model contracts, are also facing scrutiny, and this raises the question as to whether a similar challenge involving binding corporate rules could be next.

Finally, 2016 also saw the adoption of the NIS Directive, which must be implemented into national laws by May 2018. Given the increased risk of cyberattacks against organisations, it is hoped that these new provisions will strengthen the EU cyber breach strategy and reduce the risk of organised cyber crime. Organisations should review the provisions of the NIS Directive and begin amending their cybersecurity practices and procedures to ensure compliance.

65 Article 14 of the proposed NIS Directive.

Appendix 1

ABOUT THE AUTHORS

WILLIAM RM LONG

Sidley Austin LLP

William RM Long is a partner in the London office of Sidley Austin LLP and heads the EU data protection and privacy practice. He advises international clients on a wide variety of data protection, privacy, cybersecurity, e-commerce and other regulatory matters.

GÉRALDINE SCALI

Sidley Austin LLP

Géraldine Scali is a senior associate in the London office of Sidley Austin LLP whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

FRANCESCA BLYTHE

Sidley Austin LLP

Francesca Blythe is an associate in the London office at Sidley Austin LLP whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP's highly ranked privacy, data security and information law practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Data Security, Privacy &

Intellectual Property Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul has also served on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President, and currently remains an *ex officio* member. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

SIDLEY AUSTIN LLP
Sidley Austin LLP
Woolgate Exchange
25 Basinghall Street
EC2V 5HA
London
United Kingdom
Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
wlong@sidley.com
gscali@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com