The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 1

EUROPEAN UNION OVERVIEW

William Long, Géraldine Scali 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] (the Data Protection Directive), which regulates the collection and processing of personal data across all sectors of 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 couple of years with the European Commission publishing in January 2012 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. The proposal would also see significant new enforcement powers including fines of up to 5 per cent of annual worldwide turnover or €100 million, whichever is the greater.

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

---

1 William Long and Alan Charles Raul are partners and Géraldine Scali is a senior 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).

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 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 criminal offences and 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 which forms part of a filing system. The 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 Directive, which include:[4]

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;

d establishment – a controller that carries out the effective and real exercise of activity through stable arrangements in a Member State;[5]

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 relates 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

4 Article 2 of the Data Protection Directive.

5 Recital 19 of the Data Protection Directive.

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.[6] 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.[7]

Conditions for processing

Controllers may only process personal data if they have satisfied one of six conditions: (1) the data subject in question has consented to the processing; (2) the processing is necessary to enter into or perform a contract with the data subject; (3) 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; (4) the processing is necessary to comply with a legal obligation; (5) that the processing is necessary to protect the vital interests of the data subject; or (6) the processing is necessary for the administration of justice or carried out in fulfilment of a public interest function. Of these conditions the first three will be most relevant to business.[8]

Personal data that relates 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.[9] The circumstances that will often be most relevant to a business would be where the data subject has explicitly consented to the processing.

6 Article 18 of the Data Protection Directive.

7 For example in Germany, the notification requirement does not apply: (1) if the data controller has appointed a data protection officer (Section 4d(2) of the Federal Data Protection Act); or (2) 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).

8 Article 7 of the Data Protection Directive.

9 Article 8 of the Data Protection Directive.

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 purpose(s) 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).[10] In instances where the personal data is 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 is first disclosed. Also, in cases of indirect collection, it may 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 is 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.[11]

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.[12]

Prohibition on transfers outside the EEA

Controllers may not transfer personal data to countries outside of the European Economic Area (EEA)[13] unless the recipient country provides an adequate level of protection for the personal data.[14] The EU 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 EU Commission has made findings of

10 Article 10 of the Data Protection Directive.

11 Article 6 of the Data Protection Directive.

12 Article 17 of the Data Protection Directive.

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

14 Article 25 of the Data Protection Directive.

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 US has reached agreement with the EU Commission on a set of 'Safe Harbor' principles to which organisations in the US may subscribe to in order to be deemed 'adequate' to receive personal data from controllers in the EU.[15]

Where transfers are to be made to countries that are not deemed adequate other exceptions may apply to permit the transfer.[16] 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 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 it grants third-party rights to data subjects to enforce the terms of the model contract against the data exporter and data importer, and requires the parties to the model contract to give broad warranties and indemnities. The clauses of the model contracts can also not 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.

An alternative means of authorising transfers of personal data outside the EEA are 'binding corporate rules'. This approach may be suitable for multinational companies 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 DPA 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[17] on binding

15 The US–EU Safe Harbor Framework was approved in 2000. Details of the Safe Harbor Agreement between the EU and the US can be found in the EU Commission Decision 520/2000/EC. The Safe Harbor scheme is currently being reviewed by the European Commission due to the revelations concerning the NSA. On 27 November 2013, the European Commission has issued a communication on the functioning of the Safe Harbor from the perspective of EU citizens and companies established in the EU, which contains 13 recommendations designed to strengthen Safe Harbor related to transparency, redress, enforcement and access by US authorities.

16 Article 26 of the Data Protection Directive.

17 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.

corporate rules including a model checklist for approval of binding corporate rules[18] with a table with the elements and principles to be found in binding corporate rules[19].

iii Marketing

The EU Electronic Communications (Data Protection and Privacy) Directive 2002/58/EC (the 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[20] 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 such communications will require the recipient's prior consent or, alternatively can be sent without prior consent unless the recipient has 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 has also been amended in 2009[21] to require that website operators obtain the informed

---

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 (FAQa) 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 adopted on 19 April 2013.

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

19 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.

20 Unsolicited e-mails may be sent without prior consent to existing customers: (i) 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 email is for similar products or services, and (ii) if the customer has been given an opportunity to object free of charge in an easy manner to such use of his/her electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use - Article 13 (2) of the ePrivacy Directive.

21 Directive 2009/56/EC.

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: (1) when the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; and (2) where the cookie is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[22]

The Article 29 Working Party has published an opinion on the cookie consent exemption[23] which 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 which 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.[24]

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.[25]

Data subjects also have rights to object to certain types of processing where there are compelling legitimate grounds;[26] 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.

III PROPOSED EU DATA PROTECTION REGULATION

As referred to above, the current EU data protection regime is subject to review with intensive discussion on the proposed EU Data Protection Regulation (the 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. The Civil Liberties Committee also approved a mandate to start negotiations with the Council of Ministers

22 Article 5(3) of the ePrivacy Directive.

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

24 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.

25 Article 12 of the Data Protection Directive.

26 Article 14 of the Data Protection Directive.

(which represents EU Member States) and the EU Commission – the 'trilogue' process. It is possible that final agreement and adoption on the Regulation may occur in 2015.

The proposed Regulation once adopted will have a significant impact on many governments, businesses and individuals both in the EU and outside the EU. Based on the latest amendments of the European Parliament, the main elements of the proposed Regulation are summarised below.

i Enforcement

The amount of the maximum fines for non-compliance with the proposed Regulation is 5 per cent of annual worldwide turnover or €100 million, whichever is the greater, with an ability for individuals and any association, acting in the public interest, to bring claims for non-compliance.

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: (1) the offering of goods or services to EU citizens; or (2) the monitoring of such individuals. This means that many non-EU companies that have EU customers will need to comply with the proposed Regulation once implemented.

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. In case of a dispute between DPAs, action can be decided upon by the European Data Protection Board.

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 if adopted could have a major impact on how online companies market their products and services.

v Explicit consent

Consent for processing personal data should be explicit, with affirmative action required under the proposed Regulation. The mere use of a service will not amount to consent. According to the proposal, 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. Processing data on children under 13 also requires the consent of the parent or legal guardian. 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 proposed Regulation requires that certain standardised information should be provided to individuals in the form of symbols or icons similar to those used in the food industry. Individuals should also be 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.

vii Right of erasure

In the latest amendments by the European Parliament, the 'right to be forgotten' has been replaced by a 'right of erasure' giving individuals a right to have their personal data erased where the data is no longer necessary or where they withdraw consent, although certain exemptions also apply, such as where data is required for scientific research or for compliance with a legal obligation of EU law.

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 every two years. Importantly, controllers will need to implement privacy by design throughout the lifecycle of processing from collection of the data to its deletion. In addition, businesses will need to keep detailed documentation of the data being processed and carry out a privacy impact assessment where the processing presents specific risks, such as the use of health data or where the data involves more than 5,000 individuals. This assessment also has to be reviewed every two years.

ix Data protection officers

Businesses that process data on more than 5,000 people in any 12-month period, or that process sensitive data, such as health data, will also need to appoint a data protection officer who should have extensive knowledge of data protection and who does not necessarily need to be an employee.

x Security and security breaches

The controller and the processor will need to implement appropriate technical and organisational security measures. The proposal also requires that security policies contain a number of elements 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. In addition, security breaches will need to be notified to DPAs without undue delay.

xi International data transfers

In addition to binding corporate rules and other data transfer solutions, a new method allowing for international data transfers of personal data from the EU includes the use of a 'European data protection seal' awarded by European DPAs for businesses and recipients that are audited for compliance with the Regulation. The latest amendments also re-

introduce an important provision requiring that any requests for access to personal data by foreign authorities or courts outside the EU must be authorised by a DPA.

xii Health data

The Regulation also has important provisions relating to the use of health data, including the processing of personal data for scientific research, which is only permitted with consent subject to exceptions by Member States where the scientific research serves a high public interest with the data either anonymised or pseudonymised under the highest technical standards with measures to prevent re-identification of individuals.

IV CLOUD COMPUTING

In its guidance on Cloud Computing adopted on 1 July 2012,[27] the EU's Article 29 Working Party states that the majority of data protection risks can be divided into two main categories: (1) the lack of control over the data; and (2) insufficient information regarding the processing operation itself. The lawfulness of the processing of personal data in the cloud depends on the adherence to 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

In order 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 (the agreement) along with service levels and financial penalties on the provider for non-compliance.

ii Purpose Specification and limitation requirement[28]

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. In order 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 the subcontractors.

iii Security[29]

Under the Data Protection Directive, the 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

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

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

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

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 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 centers 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's standard contractual clauses.

v Erasure of data[30]

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 is erased securely at the request of the client.

vi Data subject rights[31]

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 and to ensure that the same holds true for the relation to any subcontractor.

vii International transfers[32]

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. According to the Article 29 Working Party Opinion in a

30 Article 6 (e) of Data Protection Directive.

31 Article 12 and 14 of the Data Protection Directive.

32 Article 25 and 26 of the Data Protection Directive.

cloud environment, sole-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles.

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.

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 law enforcement authority unless otherwise prohibited, such as 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[33] 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 is disclosed, except where such interests are overridden by the interests or the fundamental rights

33 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.

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.

ii Limiting the number of persons eligible for using 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 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, 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: the entity responsible for the ethics reporting programme; the acts of which he or she is accused; the departments or services that might receive the report within the company or in other entities or companies of the corporate group; and 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 jurisdiction outside the EEA for use in civil litigation[34] 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 is 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.

34 WP 158- Working Document 1/2009 on pre-trial discovery for cross-border civil litigation adopted on 11 February 2009.

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 suggests the use of binding corporate rules or the Safe Harbor regime. 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 a Network and Information Security Directive[35] (the NIS Directive), which had been proposed by the European Commission in 2013. The NIS Directive is part of the European Union's Cyber Security Strategy aimed at tackling network and information security incidents and risks across the EU.

The main elements of the proposed NIS Directive include a new national strategy, a cooperation network and certain security requirements.

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 level of network and information security.[36] This includes designating a competent national authority for information security and the setting up of a computer emergency response team that is responsible for handling incidents and risks.

ii Cooperation network

The competent authorities in EU Member States and the European Commission will form a cooperation network to coordinate against risks and incidents affecting network and information systems[37]. The cooperation network will exchange information between authorities and also provide early warnings on information security risks and incidents and agree on a co-ordinated response in accordance with an EU NIS cyber-cooperation plan.

35 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.

36 Article 5 of the proposed NIS Directive.

37 Article 8 of the proposed NIS Directive.

iii Security requirements

A key element of the NIS Directive is that Member States must ensure public bodies and certain market operators[38] take appropriate technical and organisational measures to manage the security risks to networks and information systems and which guarantee a level of security appropriate to the risks.[39] 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. According to amendments by the European Parliament the significance of the incident should take into account: (1) the number of users affected; (2) the duration of the incident; and (3) the geographic spread of the area affected by the incident.

The NIS Directive will now need to be agreed with the EU's Council of Ministers and may be adopted in 2015.

VIII OUTLOOK

The Article 29 Working Party has recently produced an opinion on topical developments on the internet of things (IoT).[40] The opinion identifies the main data protection risks that lie within the ecosystem of the IoT before providing guidance on how the EU legal framework should be applied in this context, and a comprehensive set of practical recommendations addressed to the different stakeholders concerned. That universe includes device manufacturers, application developers, social platforms, further data recipients, data platforms and standardisation bodies. The opinion is, of course, intended to help such stakeholders implement privacy and data protection in the design of their products and services.

Specific recommendations include: conduct of privacy impact assessments; using only aggregated data; applying privacy by design and privacy by default; allowing data subjects and users to exercise their rights and thus be 'in control' of the data; providing

38 Market operators are listed in Annex II of the NIS Directive as amended by the European Parliament and includes operators in energy and transport, financial market infrastructures, operators in the water production and supply and the food supply chain and internet exchange points. It should be noted that information service providers (e.g., e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores) were included in the European Commission's proposal but were removed as part of the EU Parliament's amendments.

39 Article 14 of the proposed NIS Directive.

40 WP 223 – Opinion 8/2014 on the Recent Developments on the Internet of Things adopted on 16 September 2014. As explained in this opinion, 'the concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – 'things' as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.'

methods for giving information, and offering a right to refuse, or requesting consent, that are as user-friendly as possible. Devices and applications should also be designed so as to inform users and non-user data-subjects, for example, via the device's physical interface or by broadcasting a signal on a wireless channel.

The Article 29 Working Party has also published a statement on the impact of the development of 'big data' on the protection of individuals with regard to the processing of their personal data in the EU.[41] The principles of purpose limitation and data minimisation are core concerns with respect to big data, requiring data controllers to collect personal data only for specified, explicit and legitimate purposes, and not further process such data in a way incompatible with those purposes. The Working Party acknowledges, however, that the challenges of big data will require innovative thinking on how some of these and other key data protection principles are applied in practice. The Working Party plans to initiate international cooperation with other relevant regulators in order to provide unified guidance and operational answers on the implementation of data protection rules to big data.

The growing interest in and development of areas such as the IoT, big data and cloud computing are likely to continue to be areas of intense discussion in the EU in 2015 and beyond.

41 WP 221 – Statement of the WP29 on the impact of the development of big data on the protection of individuals with regards to the processing of their personal data in the EU adopted on 16 September 2014

Appendix 1

ABOUT THE AUTHORS

WILLIAM LONG

Sidley Austin LLP

William RM Long is a partner in the London office of Sidley Austin LLP running 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.

Mr Long is a member of the European Advisory Board of the International Association of Privacy Professionals and on the DataGuidance panel of data protection lawyers. Mr Long is also a chair of the DataGuidance Financial Services Group, which includes data privacy officers from some of the world's leading financial institutions and a member of the Digital Economy Committee of the American Chamber of Commerce in Brussels examining European data protection issues.

Mr Long is also a contributor to a number of books on data protection including legal text books published by BNA in the area of privacy, cloud computing and health data. He has also been interviewed widely for his thought leadership, including in the *International New York Times* and writes for a number of publications including *Computer Weekly*, *Cloud Pro* and *CIO Today*, *E-Finance & Payments Law & Policy*, *Data Protection Law & Policy*, *Journal of Electronic Business Law*, *Journal of eCommerce Law and Policy* and *e-Health Law & Policy*. English solicitor.

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.

Ms Scali has advised international clients on the implementation of global compliance data protection and privacy projects, social media and on a broad range of data protection and privacy issues. In particular, Ms Scali has experience with regards to

cross-border transfers including binding corporate rules, cybersecurity, security breach responses, the use of whistle-blowing hotlines and cloud computing. Ms Scali also organises Women in Privacy, which is a network group of in-house counsel and data protection officers that regularly meet to discuss data protection issues.

In addition, Ms Scali regularly speaks on data protection, cybersecurity and cloud computing and writes for a number of journals, including *Data Protection Law & Policy*. Before joining Sidley Austin, Ms Scali practised in France in leading French and English law firms focusing on computer law, e-commerce, data protection, privacy and communication law. Ms Scali is a dual-qualified lawyer admitted to practise as a solicitor in the UK (England and Wales 2014) and a French lawyer admitted to the Paris Bar in 2005.

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 chairman 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 Privacy, Intellectual Property, Technology and Antitrust Litigation Advisory Committee of the National Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President. He is 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
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

www.sidley.com