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 20

UNITED KINGDOM

William Long and Géraldine Scali[1]

I OVERVIEW

Like other countries in Europe, the UK has adopted an omnibus data protection regime implementing the EU Data Protection Directive 95/46/EC (the Data Protection Directive),[2] which regulates the collection and processing of personal data across all sectors of the economy.

II THE YEAR IN REVIEW

Over the past months, cyber risk and security breaches have become almost daily news in the UK. In June 2014, as part of the UK Cyber Security Strategy,[3] the UK government launched a set of basic measures called Cyber Essentials that any organisation can use to reduce cyber risk and become certified.

Also, the UK passed the Data Retention and Investigatory Powers Act 2014, which will replace the UK Data Retention (EC Directive) Regulations 2009, which

1 William Long is a partner 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 The UK Cyber Security Strategy – Protection and promoting the UK in a digital world, November 2011.

implemented the Data Retention Directive[4] and that were declared invalid by the European Court of Justice earlier this year[5].

In 2014 big data was also a topic of major discussion, raising various data protection issues which the UK Information Commissioner's Office (ICO) addressed in a report published in July 2014.[6] In addition the ICO published a new code of practice on conducting privacy impact assessments[7] and a new code of practice on subject access.[8]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

In the UK, data protection is mainly governed by the Data Protection Act 1998 (DPA), which has implemented the Data Protection Directive into national law and entered into force on 1 March 2000.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulates direct marketing but also the processing of location and traffic data and the use of cookies and similar technologies. The PECR have implemented Directive 2002/58/EC[9] (as amended by Directive 2009/136/EC).

Key definitions under the DPA

a Data controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed;[10]

b data processor: any person (other than the employee of a data controller) who processes the data on behalf of the data controller;[11]

c data subject: an individual who is the subject of personal data;[12]

4 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

5 Court of Justice of the European Union – judgment in joined cases C-293/12 *Digital Rights Ireland* and C-594/12 *Seitlinger*.

6 ICO, Guidelines on Big Data and Data Protection, 28 July 2014.

7 ICO, Conducting Privacy Impact Assessments Code of Practice, 25 February 2014.

8 ICO, Subject Access Code of Practice: Dealing with requests from individuals for personal information, February 2014.

9 Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

10 Section 1 of the DPA.

11 Ibid.

12 Ibid.

d personal data: data that relates to a living individual who can be identified from that data, or from that data and other information that is in the possession of, or is likely to come into the possession of, the data controller;[13]

e processing (in relation to information): obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data, disclosure of the information of data by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data;[14] and

f sensitive personal data: personal data consisting of information as to the racial or ethnic origin of the data subject, his or her political opinions, his or her religious beliefs or information of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual life, the commission or alleged commission by him/her of any offence, or any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.[15]

Data Protection Authority

The DPA and PECR are enforced by the ICO. The ICO also enforces and oversees the Freedom of Information Act 2000, which provides public access to information held by public authorities.[16] The ICO has an independent status and is responsible for: maintaining the public register of data controllers; promoting good practice by giving advice and guidance on data protection and working with organisations to improve the way they process data through audits, arranging advisory visits, data protection workshops; ruling on complaints; and taking regulatory actions.

ii General obligations for data handlers

Under the DPA, data controllers must comply with the eight data protection principles[17] and ensuing obligations.

First principle: fair and lawful processing

Personal data must be processed fairly and lawfully. This essentially means that the data controller must: (1) have a legitimate ground for processing the personal data; (2) not use data in ways that have an unjustified adverse effect on the individuals concerned; (3) be transparent about how the data controller intends to use the personal data, and give the data subject appropriate privacy notices when collecting their personal data; (4) handle a data subject's personal data only in ways they would reasonably expect and consistent

13 Ibid.

14 Ibid.

15 Section 2 of the DPA.

16 Freedom of Information Act 2000.

17 Schedule 1 of the DPA.

with the purposes identified to the data subject; and (5) make sure that nothing unlawful is done with the data.

Legal basis to process personal data

As part of fair and lawful processing, the processing must be justified by at least one of six following specified grounds listed in Schedule 2 of the DPA.

The DPA applies a stricter regime in the case of sensitive personal data,[18] which may only be processed on the basis of certain limited grounds, including where the data controller has obtained the explicit consent of the data subject.[19]

Registration with the ICO

Under the DPA, a data controller who is processing personal data must make a notification with the ICO[20], unless certain limited exemptions apply. A data controller who is not established in the UK, or any other EEA state, but is using equipment in the UK for processing personal data other than merely for the purposes of transit in the UK, has to appoint a representative in the UK and provide the contact name and details of the representative to the ICO in the registration form. Notification with the ICO consists of filling in a form and the payment of a fee, which must be paid when the data controller registers for the first time and then every year when the registration is renewed.

Data protection officer

There is no current legal requirement to appoint a data protection officer.

Information notices

Data controllers must provide data subjects with information on how their personal data is being processed. In general terms, an information notice should, according to the ICO,[21] state: (1) the data controller's identity and, if the data controller is not based in the UK, the identity of its nominated UK representative; (2) the purpose(s) for which the processing of personal data is intended; and (3) any additional information the data controller needs to give individuals in the circumstances to be able to process the data fairly.[22]

Second principle: processing for specified and lawful purposes

Personal data can only be obtained for one or more specified and lawful purposes, and must not be processed in a way that is incompatible with those purposes.

18 See definition in subsection i, *supra*.

19 Schedule 3 of the DPA.

20 Section 18 of the DPA.

21 ICO, Privacy Notices Code of Practice', December 2010.

22 ICO, Guide to Data Protection, Part B 1, paragraph 25.

Third principle: personal data must be adequate, relevant and not excessive
A data controller must ensure that it holds sufficient personal data to fulfill its intended lawful purposes, but that personal data must be relevant and not excessive to those purposes.

Fourth principle: personal data must be accurate and kept up to date
Data controllers must ensure that personal data is accurate and, where necessary, kept up to date. The ICO recommends[23] data controllers to take reasonable steps to ensure the accuracy of any personal data obtained, ensure that the source of any personal data is clear, and carefully consider any challenges to the accuracy of information and whether it is necessary to update the information.

Fifth principle: personal data must not be kept for longer than necessary
Personal data processed for particular purposes should not be kept for longer than is necessary for those purposes. In practice, this means that the data controller must review the length of time it keeps personal data and consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain this information. Data controllers must also securely delete personal data that is no longer needed for this purpose or these purposes and update, archive or securely delete information if it goes out of date.

It is good practice to establish standard retention periods for different categories of information (e.g., employees' data and customer data). In order to determine the retention period for each category of information, data controllers should take into account and consider any legal or regulatory requirements or professional rules that would apply.[24]

Sixth principle: personal data must be processed in accordance with the rights of data subjects
Personal data should be processed in accordance with the rights of data subjects under the DPA. In particular, the data controller must: (1) provide information in response to a data subject's access request;[25] (2) comply with a justified request to prevent processing which is causing or will be likely to cause unwarranted damage or distress to the data subject or another person; (3) comply with a notice to prevent processing for the purposes of direct marketing; and (4) comply with a notice objecting to the taking of automated decisions.

Seventh principle: measures must be taken against unauthorised or unlawful processing of personal data
Appropriate technical and organisational measures must be taken by the data controller against unauthorised or unlawful processing of personal data and against accidental loss

23 ICO, Guide to Data Protection.

24 Ibid.

25 ICO, Subject Access Code of Practice.

or destruction of, or damage to, the personal data. Where a data controller uses a data processor to process personal data on its behalf then the data controller must ensure that it has entered into a written contract that obliges the data processor to only process the personal data on the instructions of the data controller and to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

Eighth principle: transfers of personal data to a country or territory outside the European Economic Area

See Section IV, *infra*.

iii Technological innovation and privacy law

Anonymisation

The DPA does not apply to anonymous data. However, there has been a lot of discussion over when data is anonymous and the methods that could be applied to anonymise data.

The ICO in its guidance on anonymisation[26] recommends organisations using anonymisation to have in place an effective and comprehensive governance structure that should include: (1) a senior information risk owner with the technical and legal understanding to manage the process; (2) staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them; (3) procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice; (4) knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation; (5) a joint approach with other organisations in their sector or those doing similar work; (6) use of a privacy impact assessment; (7) clear information on the organisation's approach on anonymisation including how personal data is anonymised and the purpose of the anonymisation, the techniques used and whether or not the individual has a choice over the anonymisation of its personal data; (8) review of the consequences of the anonymisation programme; and (9) a disaster-recovery procedure should re-identification take place and the individual privacy is compromised.

Big data

The DPA does not prohibit the use of big data and analytics. However, because it raises various data protection issues, the ICO has issued guidance in July 2014[27] considering data protection issues raised by big data. The ICO suggests how data controllers can comply with the DPA while using big data covering a broad range of topics including anonymisation, privacy impact assessments, repurposing data, data minimisation, transparency and subject access.

26 In November 2012, the ICO published a code of practice on managing data protection risks related to anonymisation. This code provides a framework for organisations considering using anonymisation and explains what it expects from organisations using such processes.

27 ICO, Guidelines on Big Data and Data Protection, 28 July 2014.

Bring your own device

The ICO has published guidance for companies on implementing 'bring your own device' (BYOD)[28] programmes allowing employees to connect their own devices to company IT systems. Organisations using BYOD should have a clear BYOD policy so that employees connecting their devices to the company IT systems clearly understand their responsibilities.

In order to address the data protection and security breach risks linked to BYOD, the ICO recommends that companies take various measures including considering which type of corporate data can be processed on personal devices; how to encrypt and secure access to the corporate data; how the corporate data should be stored on the personal devices; how and when the corporate data should be deleted from the personal devices; and how the data should be transferred from the personal device to the company servers.

Organisations should also install antivirus software on personal devices, provide technical support to the employees on their personal devices when they are used for business purposes and have in place a 'BYOD acceptable use policy' providing guidance to users on how they can use their own devices to process corporate data and personal data.

Cloud computing

The use of cloud computing and how it complies with EU data protection requirements has been a subject of much discussion recently. The ICO, like many other data protection authorities in the EU, has published guidance on cloud computing.[29]

Cloud customers should choose their cloud provider based on economic, legal and technical considerations. According to the ICO it is important that at the very least such contracts allow the cloud customer to retain sufficient control over the data in order to fulfill their data protection obligations.

The ICO proposes a checklist that organisations can follow prior to entering into an agreement with a cloud provider with questions around confidentiality, integrity, availability and other legal and data protection issues.[30]

Cookies and similar technologies

In 2009, the e-Privacy Directive 2002/58/EC was amended.[31] This included a change to Article 5(3) of the e-Privacy Directive requiring consent for the use of cookies and similar technologies. This new requirement was implemented in the UK through the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. As a result, organisations now have an obligation to obtain consent of website users to place cookies or similar technologies on their computers and mobile devices.[32] The consent obligation does not apply where the cookie is used 'for the sole purpose of carrying

28 ICO, Guidelines on Bring Your Own Device (BYOD), 2013.

29 ICO, Guidance on the Use of Cloud Computing, 2012.

30 See 'European Union Overview', Chapter 1 for more details on cloud computing.

31 Directive 2009/136/EC.

32 Regulation 6 of the PECR.

out the transmission of a communication over an electronic communication network' or is 'strictly necessary' to provide the service explicitly requested by the user. This exemption is applied restrictively and so could not be used when using analytical cookies. Organisations must also provide users with clear and comprehensive information about the purposes for which the information, such as that collected through cookies, is used.

The ICO has published guidance on the use of cookies, and provides recommendations on how to comply with the requirements and how to obtain consent and considers that implied opt-in consent is a valid form of consent if there is some action taken by the consenting individual form which the consent can be inferred, such as visiting the website and going from one page to another by clicking on a particular button.[33]

iv Specific regulatory areas

Employee datas

There is no specific law regulating the processing of employee data. However, the ICO has published an 'Employment practices code' and supplementary guidance to help organisations comply with the DPA and to adopt good practice.[34]

The code contains four parts covering: (1) recruitment and selection, providing recommendations with regards to the recruitment process and pre-employment vetting; (2) employment records, which is about collecting, storing, disclosing and deleting employees' records; (3) monitoring at work, which covers the employer's monitoring of employees' use of telephones, internet, e-mail systems and vehicles and; (4) workers' health, covering occupational health, medical testing and drug screening.

Employee monitoring[35]

The DPA does not prevent employers monitoring their employees. However, monitoring employees will usually be intrusive and workers have legitimate expectations that they can keep their personal lives private. Workers are also entitled to a degree of privacy in their work environment.

Organisations should carry out a privacy impact assessment before starting to monitor their employees to clearly identify the purposes of monitoring, the benefit it is likely to deliver, the potential adverse impact of the monitoring arrangement, and judge if monitoring is justified as well as take into account the obligation that arises from monitoring. Organisations should also inform workers who are subject to the monitoring of the nature, extent and reasons for monitoring unless covert monitoring is justified.

Employers should also establish a policy on use by employees of electronic communications explaining acceptable use of internet, phones and mobile devices, and the purpose and extent of electronic monitoring. It should also be outlined how the policy is enforced and the penalties for a breach of the policy.

33 ICO, Guidance on the Rules on Use of Cookies and Similar Technologies, 2012.

34 ICO, Employment Practices Code and supplementary guidance, 2011.

35 Ibid.

Opening personal e-mails should be avoided where possible and only happen where the reason is sufficient to justify the degree of intrusion involved.

Whistle-blowing hotlines

Under the DPA, the use of whistle-blowing hotlines (where employees and other individuals can report misconduct or wrongdoing) is permitted and their use is not restricted by the ICO. There is no specific UK guidance on the use of whistle-blowing hotlines. However, organisations using them in the UK will have to comply with the data-protection principles under the DPA[36].

Electronic marketing[37]

Under the PECR unsolicited electronic communication to individuals should only be sent with the recipient's consent[38]. The only exemption to this rule is known as 'soft opt-in', which will apply if the sender has obtained the individual's details in the course of a sale or negotiations for a sale of a product or service; the messages are only marketing for similar products; and the person is given a simple opportunity to refuse marketing when their details are collected, and if they do not opt out, they are given a simple way to do so in future messages. These UK rules on consent do not apply to marketing e-mails sent to companies and other corporate bodies.[39]

Senders of electronic marketing messages must provide the recipients with their names and a valid contact address.[40]

The ICO has created a direct marketing checklist, which enables organisations to check if their marketing messages comply with the law and which also proposes a guide to the different rules on marketing calls, texts, emails, faxes and mail. The ICO has also published guidance on direct marketing.[41]

Financial services

Financial services organisations, in addition to data protection requirements under the DPA, also have legal and regulatory responsibilities to safeguard consumer data under the rules of the Financial Conduct Authority (FCA), which include having adequate systems and controls in place to discharge their responsibilities.

---

36 For guidance on how to comply with data protection principles under the DPA see WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting internal accounting controls, auditing matters, fight against bribery, banking and financial crime adopted on 1 February 2006.

37 ICO, Guide to the Privacy and Electronic Communications Regulations, 2013 and Direct Marketing Guidance, 2013.

38 PECR Regulation 22(2).

39 ICO Direct Marketing Guidance, 2013.

40 PECR Regulation 23.

41 ICO Direct Marketing Guidance, 2013.

This includes financial services firms taking reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime, such as by misuse of customer data.[42]

Failure to comply with these security requirements may lead to significant financial penalties imposed by the FCA.

IV INTERNATIONAL DATA TRANSFER

Under the eighth principle of the DPA, personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.[43] The DPA provides various exemptions to permit transfers of personal data from the EEA to countries outside the EEA that do not provide an adequate level of protection including:

a Consent – with the consent of the data subject, although as the ICO comments, valid consent means the data subject must have a real opportunity to withhold their consent without inferring a penalty or to subsequently withdraw their consent. As a result, consent is unlikely to provide an adequate long-term framework in cases or repeated or structured transfer.

b Safe Harbor – where the company in the US receiving the personal data is self-certified under the US Safe Harbor scheme organised by the US Department of Commerce, which exists for transfers of personal data from the EEA and from Switzerland.

c Model contracts – where the EU's standard contractual clauses for the transfer of personal data from a data exporter in the EEA to a data importer outside the EEA (model contracts) are entered into.

d Binding corporate rules – where the data controller has entered into binding corporate rules. As the lead data protection authority, the ICO has approved the binding corporate rules of 17 organisations so far.[44]

e Adequacy assessment – where in the view of the data controller there is an adequate level of protection for the personal data to be transferred which requires an assessment of the circumstances of the transfer (such as the nature of the data, the purposes of the transfer, security measures taken etc.) and an assessment of the law in force in the country where the data is to be transferred.

f other exceptions under the DPA – (1) where it is necessary for carrying out certain types of contract or if the transfer is necessary to set up the contract; (2) where it is necessary for reasons of substantial public interest (e.g., preventing and detecting crime, national security, and collecting tax); (3) where it is necessary to protection in the vital interests of the individual (e.g., matters of life and death);

42 SYSC 3.

43 Schedule 1 of the DPA.

44 To find the list of authorised binding corporate rules by the ICO go to http://ico.org.uk/for_organisations/data_protection/overseas/binding_corporate_rules.

(4) where the personal data is part of a public register, as long as the person to whom the data is transferred complies with any restrictions on access to or use of, the information in the register; and (5) where it is necessary in connection with legal proceedings (including future proceedings not yet under way), to get legal advice or on exercising or defending legal rights.

V DISCOVERY AND DISCLOSURE

The ICO has not published any specific guidance on this topic. E-discovery procedures and the disclosure of information to foreign enforcement agencies will most of the time involve the processing of personal data. As a result, organisations will have to comply with the data protection principles under the DPA in relation to e-discovery.

In practice this will mean informing data subjects about the processing of their personal data for this purpose. Organisations will also have to have a legal basis for processing the data. In the UK, companies may be able to rely on the legitimate interest basis to disclose the personal data unless the data contains sensitive data, in which case consent of the data subject will have to be obtained or where the processing is necessary for the purposes of establishing, exercising or defending legal rights.[45]

A data transfer solution will also have to be implemented if the data is sent to a country outside the EEA that is not deemed to provide an adequate level of protection as discussed in Section IV, *supra*.

VI PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The ICO is responsible for enforcing the DPA. In case of a breach the ICO may:

a issue information notices requiring organisations to provide the ICO with specified information within a certain time period;

b issue undertakings committing an organisation to a particular course of action in order to improve its compliance;

c issue enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

d conduct consensual assessments (audits) to check organisations are complying. In the past, the ICO's audit activities have been limited to assessments carried out with the consent of the organisations concerned. Now, however, the ICO may also issue an 'assessment notice', which enables them to inspect a government department or an organisation of a designated description to see whether it is complying with the data protection principles. The ICO does not need the organisation's consent to do this if it has issued the notice;

45 Schedule 3(6)(c) of the DPA.

e issue assessment notices to conduct compulsory audits[46] to assess whether organisations processing personal data follow good practice (data protection only);

f issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010, or serious breaches of the PECR occurring on or after 26 May 2011;

g prosecute those who commit criminal offences under the DPA. The ICO liaises with the Crown Prosecution Service to bring criminal prosecutions against organisations and individuals for breaches of the DPA; and

h report to Parliament on data protection issues of concern.

The FCA also has enforcement powers and can impose financial penalties to financial services organisations for failure to comply with their obligations to protect customer data.

ii Recent ICO-led enforcement cases

The owner of a marketing company had been prosecuted for failing to notify the ICO of changes to his notification at Willesden Magistrates Court in July 2014. He was fined £4,000, ordered to pay costs of £2,703 and a £400 victim surcharge.

A man who ran a company that tricked organisations into revealing personal details about customers was ordered to pay a total of £20,000 in fines and prosecution costs, as well as a confiscation order of over £69,000 at a hearing at Isleworth Crown Court in April 2014.

In August 2014, a £180,000 monetary penalty notice was served on the Ministry of Justice for serious failings in the way prisons in England and Wales have been handling people's information.

VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA applies to a data controller established in the UK and processing personal data in the context of that establishment. It will also apply to foreign organisations not established in the UK, or in any other EEA state, but which use equipment located in the UK (e.g., a service provider processing personal data in the UK) for processing personal data otherwise than for the purposes of transit through the UK. Data controllers not established in the UK or any other EEA country and processing personal data through equipment located in the UK must nominate a representative established in the UK and comply with the data principles and requirements under the DPA.

46 For central government organisations.

VIII CYBERSECURITY AND DATA BREACHES

i Cybersecurity

Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA provides a framework for the lawful interception of communications, access to communications data, surveillance and the use of covert human intelligence sources (undercover agents) and regulating the powers of UK public bodies to carry out surveillance and investigations.

The Secretary of State has issued codes of practice relating to the exercise and performance of the powers and duties conferred or imposed under RIPA, which provide guidance on the procedures to be followed when exercising these powers and duties. Six codes of practice are currently in force.[47]

In its 'Employment practices code' and supplementary guidance, the ICO explains that interception of employees' communications without consent is allowed under RIPA, only if the interception is solely for monitoring of recording communications which: (1) involve the business entering into transactions; or (2) relate in another way to the business or take place in some other way in the course of carrying on the business. These categories cover most business communications but they do not include personal communications by employees unless they relate to the business. In addition, interceptions are also lawful under RIPA when authorised by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Under these Regulations, interception without consent is allowed if it is part of monitoring (or recording) business communications for one of the following purposes:

a to establish the existence of facts (e.g., to collect evidence of transactions such as those involved in telephone banking or to keep records of other communications where the specific facts are important, such as being able to prove that a customer has been given certain advice);

b to ascertain that the business is complying with regulatory or self-regulatory procedures (e.g., to check that workers selling financial services are giving customers the 'health warnings' required under financial services regulation);

c to ascertain or demonstrate standards that workers are achieving (e.g., to check the quality of e-mail responses sent by workers to customer enquiries);

d to show the standards workers ought to achieve (e.g., for staff training);

e to prevent or detect crime (e.g., to check that workers or others are not involved in defrauding the business);

f to investigate or detect unauthorised use of the telecommunications system (e.g., to ensure that workers do not breach the employer's rules on use of the system

47 'Code of practice for the use of human intelligence sources', 8 September 2010; 'Code of practice for the interception of communications', 8 September 2010; 'Code of practice for investigation of protected electronic information', 8 September 2010; 'Code of practice for covert surveillance and property interference', 8 September 2010; 'Code of practice for the acquisition and disclosure of communications data', 8 September 2010; and 'Interception of communications: code of practice', 12 March 2010.

for business purposes, for example by sending confidential information by e-mail without using encryption if this is not allowed. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised); and

g to ensure the security of the system and its effective operation (e.g., to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

The Data Retention and Investigatory Powers Act 2014 (DRIP Act)

On 17 July 2014, the DRIP Act received Royal Assent just three days after being presented to Parliament.

The DRIP Act is a direct consequence of the European Court of Justice decision from 8 April 2014, which declared the Data Retention Directive[48] invalid. This was on the basis that requiring the retention of the data and allowing competent national authorities to access those data constitutes in itself an interference with the fundamental right to respect for private life and with the fundamental right to the protection of personal data.

Under the DRIP Act, the Secretary of State may, by notice, require a public telecommunications operator to retain relevant communications for a period that must not exceed 12 months if he or she considers that this is necessary and proportionate for one or more of the purposes for which communications may be obtained under the Regulation of Investigatory Powers Act 2000.

The DRIP Act will replace the UK Data Retention (EC Directive) Regulations 2009, which implemented the Data Retention Directive.[49]

UK Cyber Security Strategy

In November 2011, the Cabinet Office published the UK Cyber Security Strategy entitled 'Protecting and promoting the UK in a digital world' with four objectives for the UK government to achieve by 2015: (1) tackling cyber crime and making the UK one of the most secure places in the world to do business; (2) be more resilient to cyberattacks and better able to protect our interests in cyberspace; (3) create an open, stable and vibrant cyberspace, which the UK public can use safely and that supports open societies; and (4) to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives.

In March 2013, the government launched the Cyber Security Information Sharing Partnership to facilitate the sharing of intelligence and information on cybersecurity threats between the government and industry.

48 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

49 Ibid.

The UK government has also recently developed a Cyber Essentials Scheme which aims to provide clarity on good cybersecurity practice.

Along with the Cyber Essentials Scheme, the government has published the Assurance Framework, which enables organisations to obtain certifications to reassure customers, investors, insurers and others that they have taken the appropriate cybersecurity precautions. The voluntary scheme is currently open and available to all types of organisations.

Data breaches

Under the DPA, there is no requirement to report security breaches to the ICO and the individuals involved. Although there is no legal obligation on data controllers to report security breaches, the ICO believes that serious breaches should be brought to its attention. According to the ICO, there should be a presumption to report a breach to the ICO if a significant volume of personal data is concerned and also where smaller amounts of personal data are involved but there is still a significant risk of individuals suffering substantial harm[50]. The ICO has issued various guidance on how to manage security breaches and how to make a security-breach notification.[51]

Also, under the PECR[52] and the Notification Regulation,[53] internet and telecoms service providers must report breaches to the ICO no later than 24 hours after the detection of a personal data breach where feasible.[54] The ICO has published guidance on this specific obligation to report breaches.[55]

IX OUTLOOK

The ICO is planning to introduce a privacy seal scheme by 2016. These schemes will act as a 'stamp of approval' highlighting an organisation's commitment to maintaining privacy standards. The ICO will be endorsing at least one privacy seal scheme. The schemes will be operated by an independent third party.

50 ICO, Guidance on Notification of Data Security Breaches to the Information Commissioner's Office, 27 July 2012.

51 ICO, Guidance on Data Security Breach Management, 12 December 2012 and Guidance on Notification of Data Security Breaches to the Information Commissioner's Office, 27 July 2012 and the previous version published on 27 March 2008.

52 Regulation 5A(2) of PECR.

53 Commission Regulation No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (the Notification Regulation), which entered into force on 25 August 2013.

54 Article 2 of the Notification Regulation. The content of the notification is detailed in Annex 1 to the Notification Regulation.

55 ICO, Guidance on Notification of PECR Security Breaches, 26 September 2013.

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.

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

www.sidley.com