The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

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

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 27

UNITED KINGDOM

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

I OVERVIEW

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

II THE YEAR IN REVIEW

Recent developments in UK data protection law include the commencement in March 2015 of Section 56 of the UK Data Protection Act 1998 (DPA) making it a criminal offence to pressure an individual to make a request for his or her own personal information.

In May 2015, the English Court of Appeal issued a landmark judgment against Google that could open the door to privacy litigation in the United Kingdom.[3] The case concerned the collection by Google of Safari users' browser information, allegedly without their knowledge or consent. In its opinion, the Court of Appeal held that four individuals who used Safari browsers can bring a claim for breach of privacy and that the damages claimed can include distress – even in circumstances where there is no financial loss, as this had been the

1 William RM Long is a partner, Géraldine Scali is a senior associate and Francesca Blythe is an associate at Sidley Austin LLP.

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

3 *Google Inc v. Vidal-Hall* [2015] EWCA Civ.

intention of the EU's Data Protection Directive. On 28 July, the UK Supreme Court granted Google Inc the permission to appeal part of the lower court ruling.[4] However, the appeal was withdrawn in July 2016 following an agreement being reached between the parties.

In addition, over the past few months, the Information Commissioner's Office (ICO) updated its direct marketing guidance and published new guidance on encryption and Wi-Fi location analytics.

In July 2015, only one year after the Data Retention and Investigatory Powers Act 2014 (DRIP Act) received Royal Assent (see Section III.i, *infra*), the English High Court issued a judgment declaring the Act, which provides key surveillance authority for law enforcement and intelligence authorities, to be unlawful as it was determined that a number of the provisions were incompatible with EU human rights laws. The case has since been referred to Court of Justice of the European Union (CJEU), and a preliminary opinion of the Advocate General of the CJEU has been issued that in particular questioned the safeguards under the DRIP Act. This could have a significant impact on the UK's draft Investigatory Powers Bill, which is intended to replace the DRIP Act and which permits the bulk retention of data.

Finally, in May 2016, the EU General Data Protection Regulation (Regulation) was adopted.[5] The Regulation, which aims to create a single EU-wide law on data protection, will apply from May 2018. Whether the Regulation will become applicable law in the UK, depends on whether the UK is still part of the EU in May 2018 and the agreement the UK is able to negotiate following Brexit. However, due to the wide extraterritorial scope of the Regulation, many UK companies will still need to comply with the new requirements under the Regulation.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

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

4 Google applied for an appeal to the Supreme Court on the following grounds: (1) whether the Court of Appeal was right to hold that claimant's claims for misuse of private information are tort claims for the purposes of the rules relating to service of the proceedings out of the jurisdiction; (2) whether the Court of Appeal was right to hold that Section 13(2) of the UK Data Protection Act 1998 was incompatible with Article 23 of the Data Protection Directive; and (3) whether the Court of Appeal was right to decline the application of Section 13(2) of the UK Data Protection Act 1998 on the grounds that it conflicts with the rights guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights. The Supreme Court gave permission to appeal only on points (2) and (3), and considered that point (1) did not raise an arguable point of law.

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

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulate 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[6] (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;[7]

b data processor: any person (other than the employee of a data controller) who processes the data on behalf of the data controller;[8]

c data subject: an individual who is the subject of personal data;[9]

d personal data: data that relate 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;[10]

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 or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data;[11] 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 the subject is a member of a trade union, his or her physical or mental health or condition, sexual life, the commission or alleged commission by him or her of any offence, or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.[12]

6 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.

7 Section 1 DPA.

8 Ibid.

9 Ibid.

10 Ibid.

11 Ibid.

12 Section 2 DPA.

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.[13] The ICO has independent status and is responsible for:

a maintaining the public register of data controllers;

b 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 and data protection workshops;

c ruling on complaints; and

d taking regulatory actions.

ii General obligations for data handlers

Under the DPA, data controllers must comply with the eight data protection principles[14] 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:

a have a legitimate ground for processing the personal data;

b not use data in ways that have an unjustified adverse effect on the individuals concerned;

c 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;

d handle a data subject's personal data only in ways they would reasonably expect and consistent with the purposes identified to the data subject; and

e 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 specified grounds listed in Schedule 2 to the DPA.

The DPA applies a stricter regime in the case of sensitive personal data,[15] 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.[16]

Registration with the ICO

Under the DPA, a data controller processing personal data must make a notification to the ICO[17] unless certain limited exemptions apply. A data controller who is not established in the United Kingdom, or any other European Economic Area (EEA) state, but is using equipment in the United Kingdom for processing personal data other than merely for the purposes of transit in the United Kingdom, has to appoint a representative in the United Kingdom and

13 Freedom of Information Act 2000.

14 Schedule 1 to the DPA.

15 See definition at Section III.i, *supra*.

16 Schedule 3 to the DPA.

17 Section 18 DPA.

provide the contact name and details of the representative to the ICO in the registration form. Notification of 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,[18] state the data controller's identity and, if the data controller is not based in the United Kingdom, the identity of its nominated UK representative; the purposes for which the processing of personal data is intended; and any additional information the data controller needs to give individuals in the circumstances to be able to process the data fairly.[19]

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.

Third principle: personal data must be adequate, relevant and not excessive
A data controller must ensure that it holds sufficient personal data to fulfil 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[20] data controllers 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.

18 ICO, Privacy Notices Code of Practice, December 2010.

19 ICO, Guide to Data Protection, Part B 1, Paragraph 25.

20 ICO, Guide to Data Protection.

It is good practice to establish standard retention periods for different categories of information (e.g., employees' data and customer data). 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.[21]

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:

a provide information in response to a data subject's access request;[22]

b comply with a justified request to prevent processing that is causing or will be likely to cause unwarranted damage or distress to the data subject or another person;

c comply with a notice to prevent processing for the purposes of direct marketing; and

d 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 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 process only 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[23] recommends organisations using anonymisation to have in place an effective and comprehensive governance structure that should include:

a a senior information risk owner with the technical and legal understanding to manage the process;

b staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them;

---

21 Ibid.

22 ICO, Subject Access Code of Practice, v 1.1, February 2014.

23 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.

c procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice;
d knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation;
e a joint approach with other organisations in the same sector or those doing similar work;
f use of a privacy impact assessment;
g 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 the individual has a choice over the anonymisation of his or her personal data;
h a review of the consequences of the anonymisation programme; and
i a disaster-recovery procedure should re-identification take place and the individual's 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 issued guidance in July 2014[24] 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. The guidance included three questions on which the ICO invited feedback. A summary of feedback on big data and data protection and the ICO position was published in April 2015.[25]

In addition, the Financial Conduct Authority (FCA) called in 2015 for public input on the use of big data in the general insurance sector, and has identified this as continued priority for 2016–17.[26] In its first detailed study of big data, the FCA seeks 'to better understand how Big Data affects customers and whether it fosters competition [and] […] analyse how our regulatory framework affects Big Data developments'. The agency intends to apply what it learns in the insurance industry to other sectors.

'Bring your own device' (BYOD)

The ICO has published guidance for companies on implementing BYOD[27] 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.

To address the data protection and security breach risks linked to BYOD, the ICO recommends that companies take various measures, including:

a considering which type of corporate data can be processed on personal devices;
b how to encrypt and secure access to the corporate data; how the corporate data should be stored on the personal devices;

24 ICO, Guidelines on Big Data and Data Protection, 28 July 2014.
25 ICO, Summary of Feedback on Big Data and Data Protection and ICO Response, 10 April 2015.
26 FCA, Business Plan 2016/17, 'Our Priorities'.
27 ICO, Guidelines on Bring Your Own Device (BYOD), 2013.

c how and when the corporate data should be deleted from the personal devices; and
d 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.[28]

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 cloud customers to retain sufficient control over the data to fulfil 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 on confidentiality, integrity, availability, and other legal and data protection issues.[29]

Cookies and similar technologies

In 2009, the e-Privacy Directive 2002/58/EC was amended.[30] 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 United Kingdom 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.[31] The consent obligation does not apply where the cookie is used 'for the sole purpose of carrying 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. The ICO considers that implied opt-in consent is a valid form of consent if the consenting individual has taken some action from which the consent can be inferred, such as visiting the website and going from one page to another by clicking on a particular button.[32]

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

29 See the European Union Overview chapter for more details on cloud computing.

30 Directive 2009/136/EC.

31 PECR Regulation 6.

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

iv Specific regulatory areas

Employee data

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.[33]

The code contains four parts covering:

a recruitment and selection, providing recommendations with regards to the recruitment process and pre-employment vetting;

b employment records, which is about collecting, storing, disclosing and deleting employees' records;

c monitoring at work, which covers employers' monitoring of employees' use of telephones, internet, e-mail systems and vehicles; and

d workers' health, covering occupational health, medical testing and drug screening.

Employee monitoring[34]

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 to 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.

Opening personal e-mails should be avoided where possible and should only occur 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 United Kingdom will have to comply with the data-protection principles under the DPA.[35]

33 ICO, The Employment Practices Code – Supplementary Guidance, November 2011.

34 Ibid.

35 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 whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime adopted on 1 February 2006.

Electronic marketing[36]

Under the PECR, unsolicited electronic communication to individuals should only be sent with the recipient's consent.[37] 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 his or her details are collected, and if he or she does not opt out, he or she is 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.[38]

Senders of electronic marketing messages must provide the recipients with the sender's name and a valid contact address.[39]

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, e-mails, faxes and mail. The ICO has also published guidance on direct marketing, which it updated in March 2016.[40]

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 FCA, which include having adequate systems and controls in place to discharge their responsibilities.

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.[41]

Failure to comply with these security requirements may lead to the imposition of significant financial penalties 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 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.[42] 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 consent

36 ICO, Guide to the Privacy and Electronic Communications Regulations, 2013, and Direct Marketing Guidance, V.2.2.

37 PECR Regulation 22(2).

38 ICO, Direct Marketing Guidance, V.2.2.

39 PECR Regulation 23.

40 ICO, Direct Marketing Guidance, V.2.2.

41 SYSC 3.

42 Schedule 1 to the DPA.

without incurring a penalty, or to subsequently withdraw consent. As a result, consent is unlikely to provide an adequate long-term framework in cases of repeated or structured transfer.

b EU–US Privacy Shield: US companies that self-certify under the Privacy Shield will be able to receive personal data from the EU in compliance with EU data protection requirements. The Privacy Shield was adopted on 12 July 2016 and replaces the US–EU Safe Harbor framework, which was invalidated by the CJEU in October 2015, in the iconic *Schrems* decision.[43] US companies have been able to self-certify their compliance to the Privacy Shield Principles since 1 August 2016.

c EU Model Contract Clauses: where the EU's standard contractual clauses (model contracts) for the transfer of personal data from a data exporter in the EEA to a data importer outside the EEA 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 21 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. This 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:

- where it is necessary for carrying out certain types of contract or if the transfer is necessary to set up the contract;
- where it is necessary for reasons of substantial public interest (e.g., preventing and detecting crime, national security and collecting tax);
- where it is necessary for the protection of the vital interests of the individual (e.g., matters of life and death);
- 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
- where it is necessary in connection with legal proceedings (including future proceedings not yet under way), to get legal advice or where 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.

43 Case C – 362/14 *Schrems v Data Protection Commissioner* [2014].

44 To find the list of authorised binding corporate rules by the ICO see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

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 United Kingdom, companies may be able to rely on the legitimate-interest basis to disclose personal data unless the data contain 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 the event 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 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 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 it 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;

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 on financial services organisations for failure to comply with their obligations to protect customer data.

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

46 For central government organisations.

ii Recent ICO-led enforcement cases

On 20 August 2015, Google, Inc was ordered by the ICO to remove nine search results after the ICO ruled that they linked to information about a person that was no longer relevant.

In February 2016, the ICO issued a £350,000 monetary penalty notice against a company that generates leads in relation to individuals making a claim for a PPI refund. This was the largest fine ever issued for a cold calling operation.

In April 2016, a web-based recruitment company was prosecuted for failing to notify its processing activities to the ICO and was fined £500, ordered to pay costs of £951.75 and a victim surcharge of £50.

In May 2016, an NHS trust was issued with a £185,000 monetary penalty notice for publishing an equality and diversity spreadsheet on its website that contained confidential and sensitive personal data relating to a large number of employees and that was available to and accessible by the public for a number of months.

In August 2016, a GP surgery was issued with a £40,000 monetary penalty notice for releasing confidential information about a woman and her family to her estranged ex-partner.

In August 2016, a county council was issued with a £100,000 monetary penalty notice for leaving in an unlocked cupboard files containing confidential and sensitive personal data about 100 of its social care clients.

VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

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

VIII CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The 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 for 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 that involve the business entering into transactions; or 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 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).

47 Covert Human Intelligence Sources: Code of Practice, 8 September 2010; Interception of Communications: Code of Practice, 8 September 2010; Investigation of Protected Electronic Information: Code of Practice, 8 September 2010; Covert Surveillance and Property Interference: Revised Code of Practice, 8 September 2010; Acquisition and Disclosure of Communications Data: Code of Practice, 8 September 2010; and Interception of Communications: Code of Practice, 8 September 2010.

The DRIP Act

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

The DRIP Act is a direct consequence of the CJEU decision of 8 April 2014, which declared the Data Retention Directive[48] invalid. This was on the basis that requiring the retention of 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.

One year after receiving Royal Assent, the English High Court issued a landmark judgment declaring the DRIP Act unlawful.[49] The High Court ruled that a number of the provisions in the DRIP Act were incompatible with EU human rights law. However, the ruling was suspended until 31 March 2016 to give UK legislators time to implement appropriate safeguards.

The government is currently negotiating its replacement, the Investigatory Powers Bill, which it is hoped will receive Royal Assent by the end of 2016.

The ruling on the DRIP Act has since been referred to the CJEU by the English Court of Appeal. The Advocate General of the CJEU has issued a preliminary opinion on the case, which largely asserts that the requirements set out in Digital Rights Ireland are mandatory, which would effectively uphold the original decision of the High Court in relation to the validity of the provisions of the DRIP Act. If the CJEU follows the opinion of the Advocate General, this could have a significant impact on the status of the Investigatory Powers Bill, as the current draft does not contain the requisite safeguards.

The Investigatory Powers Bill aims to grant UK enforcement bodies and intelligence agencies the power to conduct warranted interception, interference and bulk collection of communications data to assist in counter-terrorism efforts. It also extends the Secretary of State's power to require telecommunications operators to install permanent back-doors as a means to intercept encrypted data and to force them to retain communications data about their users, including web-browser history. The Investigatory Powers Bill has been met with much disapproval from human rights and civil liberties organisations for its lack of appropriate safeguards, and by virtue of the bulk collection powers it has been referred to as the 'Snooper's Charter'.

The Investigatory Powers Bill is still being debated in the House of Lords and has recently completed its third sitting at the committee stage.

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 *David & Ors v. Secretary of State for the Home Department* [2015] EWHC 2092 (Admin).

UK cybersecurity strategy

In November 2011, the Cabinet Office published the UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, with four objectives for the government to achieve by 2015:

a tackling cybercrime and making the United Kingdom one of the most secure places in the world to do business;

b to be more resilient to cyberattacks and better able to protect our interests in cyberspace;

c to create an open, stable and vibrant cyberspace that the UK public can use safely and that supports open societies; and

d 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.

The government has also recently developed the 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 organisation.

In June 2015, the government launched a new online cybersecurity training course to help the procurement profession stay safe online.

In July 2015, the government announced the launch of a new voucher scheme to protect small businesses from cyber attacks, which will offer micro, small and medium-sized businesses up to £5,000 for specialist advice to boost their cybersecurity and protect new business ideas and intellectual property.

In January 2016, the government announced plans to assist start-ups offering cybersecurity solutions. Such start-ups will be given help, advice and support through the 'Early State Accelerator Programme', a £250,000 programme designed to assist start-ups in developing their products and bringing them to market. The programme is run by Cyber London and the Centre for Secure Information Technologies, and is funded by the Government National Cyber Security Programme.

In March 2016, the government announced that the UK's new national cyber centre (announced in November 2015) will be called the National Cyber Security Centre (NCSC). The NCSC will be based in London and will open in October 2016. It is being established to help tackle cyber crime.

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 varied guidance on how to manage security breaches and how to make a security-breach notification.[51]

In addition, 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 will introduce a consumer-facing privacy-seal scheme operated by the UK Accreditation Service. This scheme will act as a 'stamp of approval', and organisations will be able to display the seal on their products as a means to highlight their commitment to maintaining privacy standards. In an update, the ICO has stated that it aims to have the scheme up and running in 2016.

The Regulation will apply in Member States from May 2018. Whether it remains directly applicable to the UK will depend on how quickly the UK serves its notice under Article 50 of the Lisbon Treaty and how quickly a withdrawal agreement can be negotiated. As such, unless a withdrawal agreement can be negotiated and unanimously agreed in under two years, it is unlikely that the UK will have left the EU before the Regulation comes into force. Accordingly, in this circumstance, the Regulation will apply in the UK from 25 May 2018.

Even if the UK were to leave the EU shortly after the Regulation comes into force, due to the extraterritorial scope of the Regulation, any UK business that processes personal data of EU citizens either through offering goods or services to such citizens, or by monitoring their behaviour (monitoring includes tracking information about data subjects, such as their preferences, attitudes or behaviours), will need to comply with the requirements of the Regulation. Further, if the UK was to adopt its own data protection rules and regulations, it would likely ensure that these comply with EU data protection laws, in order to obtain an adequacy determination from the Commission to facilitate transfers of personal data between the EU and the UK.

---

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 PECR Regulation 5A(2).

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 (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.

As such, in the short-term, there is likely to be little change in the data protection landscape, and UK organisations should continue with their preparations for the implementation of the Regulation.

Appendix 1

ABOUT THE AUTHORS

WILLIAM RM LONG

Sidley Austin LLP

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

GÉRALDINE SCALI

Sidley Austin LLP

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

FRANCESCA BLYTHE

Sidley Austin LLP

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

SIDLEY AUSTIN LLP

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