



ICLG

The International Comparative Legal Guide to: **Data Protection 2016**

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB

Bagus Enrico & Partners

Cuatrecasas, Gonçalves Pereira

Deloitte Albania Sh.p.k.

Dittmar & Indrenius

ECIJA ABOGADOS

Eversheds SA

Gilbert + Tobin

GRATA International Law Firm

Hamdan AlShamsi Lawyers & Legal Consultants

Herbst Kinsky Rechtsanwälte GmbH

Hogan Lovells BSTL, S.C.

Hunton & Williams

Lee and Li, Attorneys-at-Law

Matheson

Mori Hamada & Matsumoto

Osler, Hoskin & Harcourt LLP

Pachiu & Associates

Pestalozzi

Rossi Asociados

Subramaniam & Associates (SNA)

Wigley & Company

Wikborg, Rein & Co. Advokatfirma DA



Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
April 2016

Copyright © 2016
Global Legal Group Ltd.
All rights reserved
No photocopying

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners



General Chapter:

1	Preparing for Change: Europe's Data Protection Reforms Now a Reality – Bridget Treacy, Hunton & Williams	1
---	--	---

Country Question and Answer Chapters:

2	Albania	Deloitte Albania Sh.p.k.: Sabina Lalaj & Ened Topi	7
3	Australia	Gilbert + Tobin: Peter Leonard & Althea Carbon	15
4	Austria	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	30
5	Belgium	Hunton & Williams: Wim Nauwelaerts & David Dumont	41
6	Canada	Osler, Hoskin & Harcourt LLP: Adam Kardash & Bridget McIlveen	50
7	Chile	Rossi Asociados: Claudia Rossi	60
8	China	Hunton & Williams: Manuel E. Maisog & Judy Li	67
9	Finland	Dittmar & Indrenius: Jukka Lång & Iris Keino	74
10	France	Hunton & Williams: Claire François	83
11	Germany	Hunton & Williams: Anna Pateraki	92
12	India	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	104
13	Indonesia	Bagus Enrico & Partners: Enrico Iskandar & Bimo Harimahesa	116
14	Ireland	Matheson: Anne-Marie Bohan & Andreas Carney	123
15	Japan	Mori Hamada & Matsumoto: Akira Marumo & Hiromi Hayashi	135
16	Kazakhstan	GRATA International Law Firm: Leila Makhmetova & Saule Akhmetova	146
17	Mexico	Hogan Lovells BSTL, S.C.: Mario Jorge Yáñez V. & Federico de Noriega Olea	155
18	New Zealand	Wigley & Company: Michael Wigley	164
19	Norway	Wikborg, Rein & Co. Advokatfirma DA: Dr. Rolf Riisnæs & Dr. Emily M. Weitzenboeck	171
20	Portugal	Cuatrecasas, Gonçalves Pereira: Leonor Chastre	182
21	Romania	Pachiu & Associates: Mihaela Cracea & Ioana Iovanesc	193
22	Russia	GRATA International Law Firm: Yana Dianova, LL.M.	204
23	South Africa	Eversheds SA: Tanya Waksman	217
24	Spain	ECIJA ABOGADOS: Carlos Pérez Sanz & Lorena Gallego-Nicasio Peláez	225
25	Sweden	Affärsadvokaterna i Sverige AB: Mattias Lindberg	235
26	Switzerland	Pestalozzi: Clara-Ann Gordon & Phillip Schmidt	244
27	Taiwan	Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Rebecca Hsiao	254
28	United Arab Emirates	Hamdan AlShamsi Lawyers & Legal Consultants: Dr. Ghandy Abuhawash	263
29	United Kingdom	Hunton & Williams: Bridget Treacy & Stephanie Iyayi	271
30	USA	Hunton & Williams: Aaron P. Simpson & Chris D. Hydak	280

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

United Kingdom



Bridget Treacy



Stephanie Iyayi

Hunton & Williams

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Data Protection Act 1998 (the “DPA”), which took effect in 2000 and implements into UK law the requirements of the EU Data Protection Directive (95/46/EC) (the “Data Protection Directive”). The purpose of the DPA is to balance the rights of individuals and the commercial interests of organisations that use personal data about individuals.

1.2 Is there any other general legislation that impacts data protection?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011) (“PECR”) implement the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”). PECR regulates direct marketing by electronic means and the use of cookies and similar technologies. It also imposes sector specific breach reporting requirements, applicable to providers of public electronic communications services.

1.3 Is there any sector specific legislation that impacts data protection?

Regulated organisations within the financial services sector have a separate obligation to conduct their business activities with “due skill, care and diligence” and to “take reasonable care to organise and control [their] affairs responsibly and effectively, with adequate risk management systems”. These requirements impose additional data protection compliance obligations on data controllers within the financial services sector, in addition to the DPA.

1.4 What is the relevant data protection regulatory authority(ies)?

The Information Commissioner’s Office (the “ICO”) oversees and enforces the DPA and PECR in the UK. The current Information Commissioner, appointed in June 2009, is Christopher Graham. His term expires in June 2016, and the name of his successor will be announced imminently. The Information Commissioner is

appointed by HM The Queen, has independent status, and reports directly to Parliament. Data controllers within the financial services sector are also regulated by the Prudential Regulation Authority (the “PRA”) and the Financial Conduct Authority (the “FCA”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
“Personal data” means any data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Under the DPA, “personal data” does not include information relating to persons who are not individuals (e.g., companies or trusts).
- **“Sensitive Personal Data”**
“Sensitive personal data” means personal data relating to ethnicity, race, political or religious beliefs, trade union membership, health, sexual life and orientation, or actual or alleged criminal proceedings and convictions. Sensitive personal data are subject to increased compliance obligations due to their sensitive nature and the increased risk of harm to the individual if the data are improperly handled.
- **“Processing”**
The DPA governs the collection, use and storage of personal data and applies to both manual and computerised data and all forms of data “processing”. “Processing” means obtaining, recording or holding data, including the organisation, adaptation or alteration, retrieval, consultation or use, disclosure and blocking, destroying or erasure of personal data.
- **“Data Controller”**
The DPA defines a “data controller” as a natural or legal person who, alone or jointly, determines the purposes for which, and the manner in which, the personal data are processed. The DPA only applies to data controllers.
- **“Data Processor”**
A “data processor” is defined as any natural or legal person (other than an employee of the controller) who processes personal data on behalf of the controller. A data processor does not have any direct statutory obligations under the DPA and is only subject to contractual obligations imposed by the data controller.

■ “Data Subject”

A “data subject” is the individual who is the subject of the personal data.

- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*

There are no other key definitions in particular.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

■ Transparency

Under Principle 1 of the DPA, personal data must be processed fairly and lawfully. Specifically, data subjects must be informed by the data controller of how their personal data will be used.

As a minimum, at the time of collection of the personal data or before it is first processed by the data controller, the data controller must provide notice of: (i) its identity; (ii) the fact that personal data are collected and the types of personal data collected; (iii) the specific purposes for which the personal data will be processed; and (iv) any further information required to make the processing fair in the particular circumstances, e.g., disclosures of the personal data to third parties or transfers of the personal data outside of the jurisdiction.

Notice should be clear, easily understandable and genuinely informative.

■ Lawful basis for processing

For personal data to be processed lawfully, the data controller must have a legal basis for each processing activity. The DPA sets out legal bases for the processing of personal data in Schedule 2, and for sensitive personal data in Schedule 3.

The legal bases commonly relied upon by UK data controllers to process personal data are: (i) consent of the data subject; (ii) processing that is necessary to perform a contract, or to enter into a contract, with the data subject; (iii) processing that is necessary to comply with a legal obligation of the data controller (other than a contractual obligation); and (iv) processing that is necessary for the legitimate interests of the data controller or a third party to whom the data are disclosed, except where it would prejudice the fundamental rights and freedoms of the data subject (this is a balancing test).

Where processing sensitive personal data, UK data controllers commonly rely on explicit consent or compliance with an employment law obligation.

■ Purpose limitation

Under Principle 2 of the DPA, personal data may only be obtained for one or more specified and lawful purposes, and cannot be further processed in any manner incompatible with that purpose. Determining whether a further purpose is “compatible” with the original purpose is a question of fact. Where a further purpose is deemed incompatible with the original purpose, the data controller must provide notice of the further purpose and be able to rely on a legal ground for the further purpose.

■ Data minimisation

Under Principle 3 of the DPA, personal data must be relevant and not excessive in relation to the purpose for which they are processed. Data controllers are therefore under a duty to process only the personal data necessary for the relevant processing purpose, and to refrain from collecting or retaining unnecessary or irrelevant personal data.

■ Proportionality

As part of the data minimisation principle, personal data collected and processed should be proportionate to the processing purposes. In practice, this means processing the least amount of personal data necessary for the purposes, and using anonymous or pseudonymous data where possible.

■ Retention

Under Principle 5 of the DPA, personal data must not be retained for longer than is necessary for the processing purpose. Data controllers must ensure that data are only collected, used and retained to satisfy the relevant processing purpose. The DPA does not, however, stipulate any specific retention periods.

■ *Other key principles – please specify*

The DPA also requires data controllers to ensure that the personal data they process are accurate and up to date (Principle 4 – see Section 4), processed in accordance with the rights of affected data subjects (Principle 6 – see Section 4), safeguarded by appropriate organisational and technical measures (Principle 7 – see Section 13), and not transferred outside of the European Economic Area (“EEA”), unless an adequate level of data protection exists (Principle 8 – see Section 8).

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ Access to data

A data subject has the right to submit a subject access request (“SAR”) to a data controller, requiring the data controller to: (i) confirm whether it is processing the data subject’s personal data; (ii) provide a description of their personal data held by the data controller, the purpose for which their data are held, the persons or category of persons to whom their data may be disclosed, and any information about the source of the data; and (iii) provide a copy of their personal data. SARs must be made in writing, and data controllers are permitted to charge a statutory fee (currently £10) towards the costs of responding to the SAR.

■ Correction and deletion

Under the DPA, personal data must be accurate and, where necessary, kept up to date (Principle 4), and must not be retained for longer than is necessary (Principle 5). A data subject can require a data controller to correct or supplement inaccurate or incomplete personal data held about them. Data subjects can also apply for a court order requiring the data controller to rectify, block, erase or destroy personal data that are inaccurate.

■ Objection to processing

A data subject has the right to object to processing, but only if it causes unwarranted and substantial damage or distress. If it does, the data subject has the right to require an organisation to stop (or not to begin) the processing. The right to object to processing is not an absolute right. In certain limited circumstances, data controllers may be required (including by court order) to stop or not begin processing a data subject’s personal data. If, in the circumstances, the data controller is not required to stop (or not begin) the processing, the data controller must provide an explanation to the data subject as to why it does not have to, and will not, stop the processing.

■ Objection to marketing

Under the DPA, a data subject can object at any time to the processing of their personal data for marketing purposes. This is an absolute right.

■ **Complaint to relevant data protection authority(ies)**

Individuals may raise complaints with the ICO. The ICO's website provides a number of survey-style complaint forms, based on different areas of complaint, currently including nuisance marketing text messages and telephone calls. The ICO encourages individuals to use these standard online complaint forms and reporting tools. Nevertheless, data subjects can also raise complaints in writing, by email, or by telephoning the ICO. There is no charge to submit a complaint.

■ *Other key rights – please specify*

Data subjects also have rights in relation to direct marketing and cookies (see Section 7).

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Under the DPA, a general registration requirement is imposed on data controllers. Certain exemptions apply, including: (i) for not-for-profit organisations, in certain circumstances; (ii) processing personal data for personal, family, or household affairs (the “domestic purposes exemption”); and (iii) data controllers who only process personal data for purposes of their own business relating to staff administration, advertising, marketing and public relations, and accounts and records.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Registrations must be submitted for each legal entity. Each data controller that is under a duty to register must submit a registration which sets out its data processing activities.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Organisations subject to the DPA and not benefitting from one of the registration exemptions must register with the ICO. This therefore includes both UK organisations and foreign organisations. The latter can register through a UK branch office or an appointed UK representative.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The following information must be included in the ICO registration: (i) name and address of the data controller (or if the data controller has nominated a representative, the name and address of the

representative); (ii) legal status of the data controller (e.g., sole trader, company); (iii) sector in which the data controller operates; (iv) nature of work; (v) description of the personal data being or to be processed, and a description of the category or categories of data subject to which they relate; (vi) processing purposes; (vii) description of any recipient(s) to whom the data controller intends or may wish to disclose the data; (viii) data transfers; and (ix) description of the data controller's security measures. There are also a number of tick-box compliance questions to complete and contact details for queries must be provided.

5.5 What are the sanctions for failure to register/notify where required?

Failure to register with the ICO is a criminal offence and may lead to a fine of up to £5,000 in a magistrates' court or an unlimited fine in the Crown Court.

5.6 What is the fee per registration (if applicable)?

An initial fee and annual renewal fee apply. Data controllers with over 250 employees and a turnover of £25.9 million or more must pay a notification fee of £500. All other data controllers must pay a £35 fee. Registered charities and small occupational pension schemes are subject to the £35 fee, regardless of their size and turnover.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

Registrations must be renewed annually.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

No processing activities require prior approval from the ICO. However, a data controller may wish to approach the ICO informally before implementing a new processing activity, particularly if it is high-risk, novel, or uses emergent technology, the compliance of which may be something of a “grey area”.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is no statutory requirement to appoint a Data Protection Officer in the UK. In practice, however, many organisations do so, particularly larger organisations.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Voluntarily appointing a Data Protection Officer does not provide statutory exemptions from other obligations. However, it affords obvious practical compliance advantages in terms of specialist knowledge and know-how, a single contact point for data protection queries, and a designated individual with overall responsibility and oversight for data protection matters.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no particular qualifications prescribed by law. In practice, Data Protection Officers typically have experience in information management, records management, IT, data security, and/or compliance.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

There are no responsibilities prescribed by law. In practice, the Data Protection Officer is typically responsible for: responding to queries and requests from data subjects, the ICO, the FCA and the PRA; developing internal policies and procedures; developing staff training; advising on compliance with applicable law; reviewing and advising on new products or procedures; identifying risk areas; and advising on legal developments that may impact the organisation.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No. However, a contact person needs to be designated on the ICO registration, and this can be the Data Protection Officer.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Postal marketing communications are not specifically regulated, but must generally comply with the requirements of the DPA.

PECR distinguishes between live telephone calls and automated recorded calls. Live unsolicited marketing calls can be made unless the number has opted-out. Companies must therefore consult the Telephone Preferences Service, the central opt-out register, and must not call any number where the person has otherwise objected to receiving their calls. Further, organisations must always identify the caller, and provide a contact address or freephone contact number if asked.

Automated pre-recorded marketing calls require specific, prior opt-in consent. Consent to receive live calls is not sufficient as a consent to receive recorded calls. Automated calls must say who is calling and provide a contact address or freephone number.

The sending of email or SMS text message marketing requires prior opt-in consent. A limited exception, known as the “soft opt-in”,

allows an organisation to send an unsolicited email or SMS text message marketing communication if: (i) the organisation obtained the recipient’s contact details in the course of a sale or negotiations for the sale of a product or service; (ii) the marketing communication relates to similar products and services; and (iii) the recipient is given a simple means of refusing the receipt of further marketing communications (e.g., an “unsubscribe” link or replying “STOP” to an SMS text message).

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The ICO actively encourages members of the public to report nuisance and unwanted marketing. Recent enforcement actions include monetary penalty notices in February 2016 of £350,000 issued to Prodiad Ltd, a lead generation firm responsible for over 46 million automated nuisance calls (the ICO’s largest ever fine) and of £80,000 issued to UKMS Money Solutions Limited, a PPI claims company, for sending more than 1.3 million spam texts.

7.3 Are companies required to screen against any “do not contact” list or registry?

Yes. A do-not-call list containing the telephone numbers of individuals who have opted-out of receiving calls for direct marketing purposes, known as the Telephone Preference Service List, is in place. In addition, the Corporate Telephone Preference Service List contains a list of business telephone numbers that have opted-out of receipt of calls for direct marketing purposes. Individuals included on such lists must not be called for marketing purposes unless the caller has received specific consent to do so.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalty for sending marketing communications in breach of PECR is a civil monetary penalty of up to £500,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Cookies and similar technologies require notice and prior opt-in consent, except where the cookie is strictly necessary for the transmission of a communication over an electronic communications network or for a service requested by the user. The “strictly necessary” exemption is narrowly interpreted and only covers a limited number of cookies.

The law does not stipulate different types of consent for different types of cookies. In practice, however, the ICO distinguishes between more and less intrusive cookies, and is more focused on the compliance of intrusive cookies such as tracking and advertising cookies, and is less focused on analytic and functional cookies.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

Consent for cookies can be implied, where sufficiently informed.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The ICO has written to a number of organisations asking them how they comply with the cookie rules, but has not to date taken any enforcement action in relation to cookies. The ICO has given cookies a low consumer-threat rating compared with unwanted marketing calls and SMS text messages.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is £500,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Transfers of personal data from the UK to outside of the EEA are generally prohibited, unless an adequate level of data protection is assured or a relevant derogation applies. A “transfer” includes the ability to access data from outside of the UK, e.g., viewing it on a computer screen from another country.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Adequacy can be established on the basis of: (i) a European Commission adequacy finding in respect of that country or otherwise covering that transfer; (ii) the exporting organisation making its own adequacy assessment; or (iii) the data exporter adducing adequate safeguards, including the use of Commission-approved standard contractual clauses or binding corporate rules (“BCRs”). Note that the U.S. Safe Harbor was declared invalid by the Court of Justice of the European Union in 2015, and at the time of writing details of the Privacy Shield, incorporating greater protections for European citizens and imposing more stringent requirements on companies, are awaiting approval.

Where an adequate level of data protection is not assured, personal data may only be transferred where a relevant derogation applies, including the unambiguous consent of the individual and transfers necessary for legal proceedings, to protect the public interest, or to protect the vital interests of the individual.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Transfers of personal data must be included in the exporting organisation’s general registration with the ICO, but do not require prior approval.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There is no UK specific statute or guidance on hotlines restricting the scope of hotlines. However, hotlines must generally comply with the requirements of the DPA. The Article 29 Working Party opinion on the application of EU data-privacy rules to internal whistle-blowing schemes has application as non-binding general guidance only.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

As there is no UK specific statute or guidance, anonymous reporting is not strictly prohibited or strongly discouraged under binding guidance. However, it is strongly discouraged under the Article 29 Working Party opinion.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Hotlines do not require separate registration or prior authorisation. However, organisations can choose to include their hotline in their ICO registration.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Employees should be informed of the existence of, the purposes served by, and the rights associated with a whistle-blowing hotline before it is implemented. Specifically, the notice should provide information regarding the scope of the hotline, how it should be used and the handling of complaints, including any rights that an employee may have in, and to, the data. Whilst whistle-blowing hotlines do not strictly require a separate privacy notice in the UK, it is recommended. In any event, the information should be provided in writing, for evidential purposes.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Only to the extent required under the terms of any trade union agreement in place.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Use of CCTV does not require prior authorisation or separate registration, but must be specifically mentioned in the general registration.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is subject to the general requirements of the DPA. Additionally, the Regulation of Investigatory Powers Act 2000 (“RIPA”) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (“LBP Regulations”) apply where data are accessed or reviewed in the course of transmission.

RIPA has the potential to cover the interception by an employer of an employee’s use of email, text messaging, instant messaging, telephone and the Internet. It is generally an offence to intercept any communication without consent.

Under the LBP Regulations, interception may be authorised in the following circumstances: (i) monitoring business communications to ascertain whether business standards are being complied with and establishing the existence of facts; (ii) national security; (iii) preventing or detecting crime; (iv) detecting unauthorised use; or (v) ensuring the effective operation of the system. The broad grounds for lawful interception without consent provided in the LBP Regulations are restricted by the requirement that the interception must be effected solely for the purposes of monitoring of communications that are relevant to the business, i.e., the LBP Regulations do not cover the interception of any personal communications of employees.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Accessing and reviewing an employee’s communications, files, work laptops, etc., is generally prohibited unless the consent of the employee is obtained. Employee monitoring can be conducted in limited circumstances without consent if there are appropriate policies and procedures in place notifying employees that accessing, monitoring or reviewing may take place. Such notice may be provided by means of a separate monitoring/electronic communications policy or included in an employee handbook, and should clearly define the nature and extent of potential monitoring. Under Section 29 of the DPA, personal data processed for the prevention or detection of crime are exempt from the requirement to give notice of the monitoring and the requirement to provide individuals with access to personal data. Devices owned personally by an employee may only be seized by an employer if the prior consent of the owner has been obtained, or a court order allowing the employer to carry out such seizure has been obtained.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Only to the extent required under the terms of any trade union agreement in place.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Processing personal data in the cloud is permitted. The ICO published cloud computing guidance in September 2012 which emphasises that the general requirements of the DPA equally apply in the context of cloud processing. The guidance prompts data controllers using cloud services to consider whether such usage could result in processing additional personal data, e.g., usage statistics and transaction history metadata. The guidance specifically advises data controllers using cloud services to: create a clear record of the categories of personal data in the cloud; select an appropriate cloud provider, particularly in terms of confidentiality and integrity of the data; and be wary of “take it or leave it” standard terms, which may not be fully compliant with the requirements of the DPA. The guidance specifically advises data controllers using cloud services to: (i) create a clear record of the categories of personal data in the cloud; (ii) select an appropriate cloud provider, particularly in terms of confidentiality and integrity of the data; and (iii) be wary of “take it or leave it” standard terms, which may not be fully compliant with the requirements of the DPA.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific terms that must be imposed on cloud providers, in addition to the general contractual obligations (of data security and use limitation).

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Big data and analytics are permitted. Where data are anonymous, the DPA does not apply. The ICO issued a binding code of practice on anonymisation in November 2012. Under the code of practice, data are considered to be anonymous and no longer personal data where the data: (i) could not be re-identified by a reasonably competent third party having access to resources and using other available information; and (ii) are essentially “put beyond use” by the data controller itself and will not be later re-identified by the data controller.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The DPA requires data controllers to put in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The level of security must be appropriate given the nature of the data (i.e., a higher level of security for sensitive personal data) and the potential risk of harm to data subjects if the security safeguards were breached. Specific standards are not stipulated by law or binding guidance, however, the ICO expects organisations to have internal controls, including: appropriate policies and procedures; access controls; training and awareness; and technical controls, including: (i) password-protected devices; (ii) use of encryption technologies; and (iii) secure disposal of IT assets.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no general legal requirement to report data breaches under the DPA. However, the ICO expects data controllers to report significant breaches to its office and will take any failure to do so into account in determining any applicable monetary penalty.

PECR contains breach reporting requirements that apply specifically to providers of public electronic communication services (e.g., Internet service providers and telecommunication providers), under which they must report breaches to the ICO via a secure PECR security breach notification web form within 24 hours of becoming aware of the breach. As soon as a service provider has enough information to confirm that there has been a breach and provide some basic facts, they must notify, even if they cannot yet provide full details. The initial notification must always include the following summary information: (i) name of the service provider; (ii) name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) date and time of the breach (or an estimate) and the date and time of detection; (iv) circumstances of the breach (e.g., theft, loss, copying); (v) nature and content of the personal data concerned; (vi) security measures applied (or to be applied) to the affected personal data; and (vii) details of the use of other providers (where applicable).

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no general legal requirement to notify affected data subjects of data breaches under the DPA. However, the ICO expects data controllers to report significant breaches to affected data subjects, particularly where there is a risk of harm and there are steps that data subjects could take to mitigate the potential harm.

13.4 What are the maximum penalties for security breaches?

The maximum penalty is £500,000.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Monetary penalty notices	Up to £500,000 for serious breaches of the DPA and PECR.	This is not applicable.
Undertakings	While the ICO has no formal powers of undertakings under the DPA, in practice the ICO requests organisations to give undertakings, committing to a particular course of action in order to improve their compliance with the DPA.	This is not applicable.
Enforcement notices	The ICO can issue enforcement notices and “stop now” orders for breaches of the DPA, requiring organisations to take specified steps in order to ensure they comply with the law.	This is not applicable.
Prosecution	This is not applicable.	The ICO liaises with the Crown Prosecution Service to bring criminal prosecutions against organisations and individuals for breaches of the DPA.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The ICO is regarded as a pragmatic rather than punitive regulator, and sees its role as educating organisations and the public on the DPA and other relevant legislation, as well as enforcing it. Nevertheless, the ICO will take action to ensure organisations meet their data protection obligations, including monetary penalties, enforcement notices, and prosecutions.

Examples of recent enforcement action brought by the ICO include:

- **Failure to register:** In July 2014, a legal advice company, Global Immigration Consultants Limited, was prosecuted for failing to notify with the ICO. It was fined £300, and ordered to pay costs and a victims’ surcharge.
- **Serious data security breach:** The Crown Prosecution Service was fined £200,000 by the ICO in November 2015 after laptops containing videos of police interviews were stolen from a private film studio. The ICO ruled that the CPS was negligent when it failed to ensure the videos were kept safe and did not take into account the substantial distress that

would be caused if the videos were lost. In February 2014, the ICO fined the British Pregnancy Advice Service, a not-for-profit charity, £200,000 for a security flaw on its website that led to the data of over 10,000 women being accessed by a hacker. In January 2013, the ICO issued Sony Computer Entertainment Europe Limited with a monetary penalty of £250,000 in relation to a serious hacking incident.

- **Persistent errors in use of personal data:** In November 2012, Prudential Assurance Company was issued with a monetary penalty of £50,000 for repeatedly confusing two customers' accounts with the same name.
- **Unlawful spamming:** In February 2016, the ICO issued a fine of £350,000 issued to Prodiad Ltd, a lead generation firm responsible for over 46 million automated nuisance calls (the ICO's largest ever fine) and of £80,000 issued to UKMS Money Solutions Limited, a PPI claims company, for sending more than 1.3 million spam texts. In November 2012, monetary penalties amounting to £440,000 (overruled on appeal) were served on two individuals who owned a marketing company which had sent millions of unlawful spam texts to the public over a three-year period. Other recent ICO fines for breaches of the marketing rules include a £90,000 fine issued to Kwik Fix Plumbers Limited for continually making nuisance calls to vulnerable victims, and a £70,000 fine issued to Parklife Manchester Ltd for sending unsolicited marketing text messages.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The disclosure of personal data and the transfer of personal data are both processing activities requiring notice and a valid legal basis. Companies typically provide a general notice at the time of collection, e.g., stating in their privacy policies that the collected personal data may be disclosed in relation to legal proceedings or in response to law enforcement access requests. For non-sensitive personal data, UK companies typically rely on the legitimate interest basis to disclose the data. For sensitive personal data, UK companies typically try to obtain the explicit consent of the affected data subjects.

15.2 What guidance has the data protection authority(ies) issued?

The ICO has not issued specific guidance on this issue. The Article 29 Working Party Working Document on pre-trial discovery for cross-border civil litigation has application as non-binding general guidance.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Nuisance calls and spam texts remain a continuing concern for consumers and a key area of action for the ICO. The ICO has issued civil monetary penalties totalling approximately £1,056,000 since April 2015, with £370,000 total penalties being issued in November 2015 alone. In January 2016, the ICO had over 100 cases under investigation, and issued 52 third party information notices. Recent enforcement actions include monetary penalty notices in February 2016 of £350,000 issued to Prodiad Ltd, a lead generation firm responsible for over 46 million automated nuisance calls (the ICO's largest ever fine) and of £80,000 issued to UKMS Money Solutions Limited, a PPI claims company, for sending more than 1.3 million spam texts. The ICO also fined Direct Security Marketing Ltd £70,000 in February 2016 for making almost 40,000 automated calls in just one day in an attempt to sell burglar alarms, almost 10,000 of which were made between 1am and 6am.

Enforcement action for data breaches is another enforcement trend. For examples of recent cases of enforcement action taken by the ICO for failure to comply with Principle 7 of the DPA, see question 14.2. Other notable fines include Staysure.co.uk, an online holiday insurance company, fined £175,000 by the ICO after IT security failings let hackers access more than 5,000 customer records, and the British Pregnancy Advice Service, a not-for-profit charity, fined £200,000 for a security flaw on its website that led to the data of over 10,000 women being accessed by a hacker.

16.2 What "hot topics" are currently a focus for the data protection regulator?

EU General Data Protection Regulation and the Directive on data protection and law enforcement: With final drafts due in the first few months of 2016, the ICO is now stepping up its work to understand the implications of the new legislation and what more it will need to do to prepare for implementation in order to understand the guidance and advice data controllers may need, and how the new regulatory process will need to work.

Privacy seals: The ICO is developing a privacy seal certification which will enable organisations which have been awarded a privacy seal to use the seal externally to show that they are demonstrating best practice when processing personal data. It will function as a trust mark. The ICO is working with the UK Accreditation Service ("UKAS") and other stakeholders to develop a framework criteria to select privacy seal scheme operators to which an organisation will make its application for a privacy seal.

Release of consumer data: Another government initiative, the Midata programme, encourages the release of consumer data back to individuals in reusable form. Bank customers can now download a file of their financial transactions and use this to find the best current account for them, and this is now being adopted by energy providers. The ICO is actively advising on the programmes' privacy concerns.

**Bridget Treacy**

Hunton & Williams
30 St Mary Axe
London, EC3A 8EP
United Kingdom

Tel: +44 207 220 5600
Fax: +44 207 220 5772
Email: btreacy@hunton.com
URL: www.hunton.com

Bridget Treacy leads Hunton & Williams' UK Privacy and Cybersecurity team and is also the Managing Partner of the firm's London office. Her practice focuses on all aspects of privacy, data protection, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. Bridget's background in complex technology transactions enables her to advise on the specific data protection and information governance issues that occur in a commercial context. Bridget is the editor of the specialist privacy journal, *Privacy and Data Protection*, and has contributed to a number of published texts. According to *Chambers UK*, "she is stellar, one of the leading thinkers on data protection, providing practical solutions to thorny legal issues".

**Stephanie Iyayi**

Hunton & Williams
30 St Mary Axe
London, EC3A 8EP
United Kingdom

Tel: +44 207 220 5608
Fax: +44 207 220 5772
Email: siyayi@hunton.com
URL: www.hunton.com

Stephanie Iyayi is an Associate in Hunton & Williams' UK Privacy and Cybersecurity team. She advises clients on all areas of UK and EU data protection law. Stephanie works on large multi-jurisdictional data protection compliance projects, including data breach incidents, employee monitoring and data retention, cross-border data transfers and other technology, media and telecommunications matters.



Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global*, *Chambers Europe* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal's* "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

This article presents the views of the author(s) and do not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.

This article appeared in the 2016 edition of The International Comparative Legal Guide to: Data Protection published by Global Legal Group Ltd, London. www.iclg.co.uk

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks



59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk