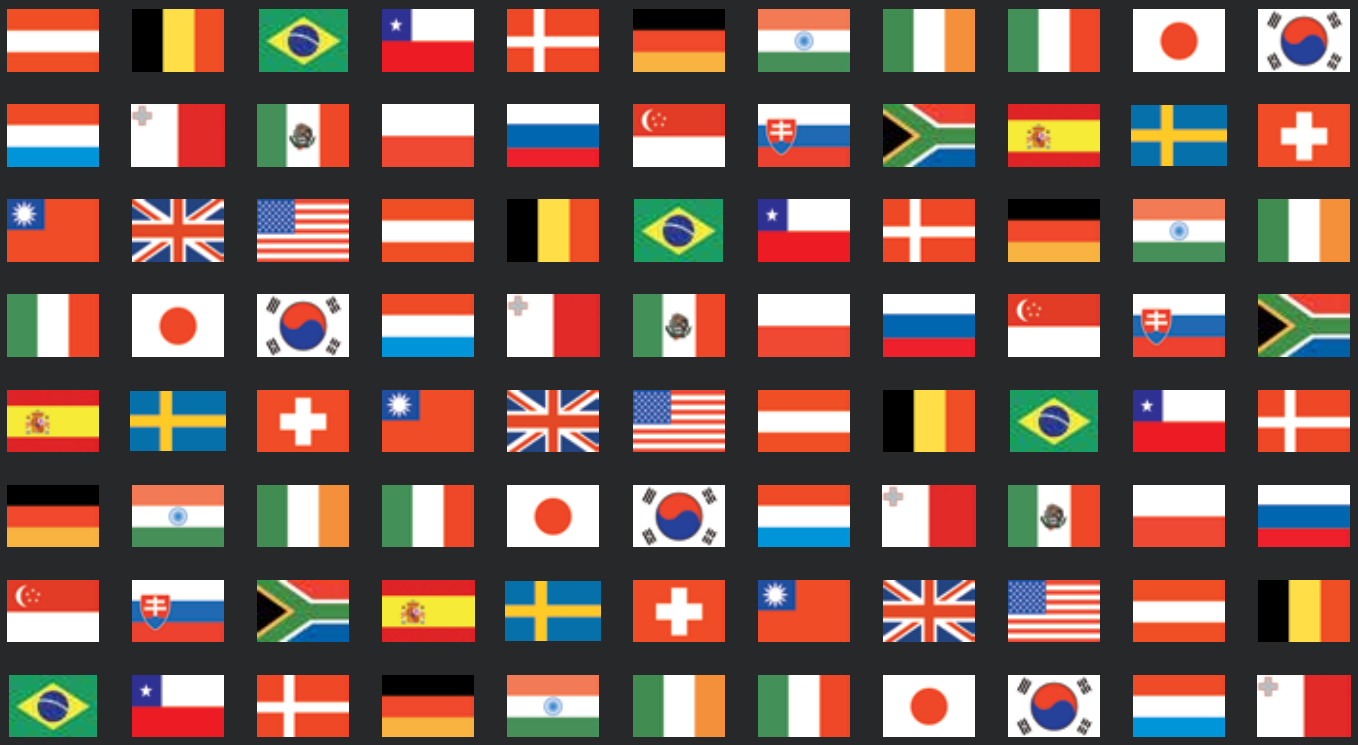
Data Protection & Privacy

Contributing editor
Rosemary P Jay



2016

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2016

Contributing Editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@lbresearch.com

Adam Sargent
adam.sargent@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Fourth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

United Kingdom

Rosemary P Jay
Hunton & Williams

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The primary legal instrument is the Data Protection Act 1998 (DPA), which implements Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of PII and the free movement of data. It is supported by secondary legislation made by statutory instrument, for example, setting fee levels for access rights. The United Kingdom has incorporated the Convention rights under the European Convention on Human Rights into law in the Human Rights Act 1998 and some privacy rights have been developed by the courts as a result of the application of that Act. The UK is a signatory to Treaty 108 of the Council of Europe. The UK has no national constitutional privacy provisions but is bound by the EU Charter of Fundamental Rights.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The DPA is supervised by the Information Commissioner's Office (ICO) appointed under the DPA. The ICO may:

- seek entry to premises subject to a warrant issued by a court;
- require the provision of information by service of information notices;
- by notice, require government departments to undergo mandatory audit (referred to as 'assessment');
- conduct audits of private sector organisations with the consent of the organisation;
- impose mandatory orders on data owners (those who control PII) requiring them to take such steps as he or she sets out in the order; and
- impose fines of up to £500,000 for serious breaches of the DPA.

All of the orders made by the ICO may be appealed. The ICO also has specific powers under secondary legislation dealing with electronic marketing to make orders in relation to notice of breaches of security by providers of electronic communication services.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

A number of breaches may lead to criminal penalties. The following may constitute criminal offences:

- failure by a data owner, where required, to register and maintain an accurate entry in the register;
- failure to comply with a mandatory enforcement or information notice under the DPA within the specified time; and
- obstructing execution of a warrant of entry or failing to cooperate or providing false information.

Further, a person who procures the disclosure of PII or discloses PII without the consent of the data owner or sells or offers for sale PII obtained without such permission commits a criminal offence.

Criminal offences can be prosecuted by the ICO or by or with the consent of the Director of Public Prosecutions.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Exemptions from the full rigour of the law apply in some circumstances and for some instances of processing. A wide exemption applies to processing by individuals for personal and domestic use but no sectors or institutions are outside the scope of the law. Recent European case law has clarified that this exemption applies only to 'purely domestic' activities.

The DPA applies to public and private sector bodies.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended), although the DPA often applies to the same activities, to the extent that they involve the processing of PII. The retention of PII by electronic service providers is regulated by the Data Retention (EC Directive) Regulations 2009. Interception and state surveillance are covered by the Regulation of Investigatory Powers Act 2000. The interception of business communications is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 made under the Regulation of Investigatory Powers Act 2000.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

The law includes many provisions dealing with information; for example, the regulation of credit files is covered in the Consumer Credit Act 1974. Laws on e-commerce include provisions linked to the regulation of PII. Laws on defamation, copyright and computer misuse also affect data protection. However, there is no specific data protection sectoral legislation. The UK has a range of 'soft law' instruments, such as codes of practice for medical confidentiality or the management of information held for policing, that apply in specific sectoral areas.

A code of practice made under the DPA applies to the sharing of PII between data owners.

7 PII formats

What forms of PII are covered by the law?

The DPA covers PII held in electronic form plus such information held in structured files, called 'relevant filing systems'. In order to fall within this

definition the file must be structured by reference to individuals or criteria relating to them, so that specific information about a particular individual is readily accessible.

Ultimately, whether a manual file is part of a relevant filing system is a matter of fact as well as law, and must be considered on a case-by-case basis.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

Organisations that are data owners ('data controllers' under the DPA) fall within the scope of the law if they are established in the UK and process PII in the context of that establishment, or if they are not established in the European Economic Area (EEA) but make use of a 'means' of processing in the UK to process PII (other than for purposes of mere transit of PII through the UK). A 'means' of processing includes equipment used to process PII, or a 'data processor'. A 'data processor' is an organisation that carries out outsourced processing of PII on behalf of a data owner.

A data owner is 'established' in the UK if it is resident in the UK, is incorporated or formed under the laws of England and Wales, Scotland or Northern Ireland, or maintains an office, branch, agency or other regular practice in the UK.

Data owners established outside the UK but using a means of processing in the UK are obliged to nominate a representative in the UK.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

The DPA is applicable to data owners only (ie, those that decide the means and purposes of the data processing). Data processors (who merely process PII at the behest of data owners) have no direct legal obligations under the DPA.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The DPA sets out different grounds for legitimate processing depending on whether the PII are non-sensitive or sensitive.

The grounds for processing non-sensitive PII are:

- consent of the individual;
- performance of a contract to which the individual is party;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-EU jurisdiction is not sufficient for the purposes of this ground);
- protection of the vital interests of the individual (ie, a life or death situation);
- the processing is necessary for carrying out public functions; or
- the processing is necessary for the legitimate interests of the data owner (or third parties to whom the PII is disclosed), unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

Distinct grounds for legitimate processing apply to the processing of sensitive PII. 'Sensitive' PII is defined as PII relating to:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health;
- sex life;
- commission or alleged commission of any offence; or
- any proceedings for committed or alleged offences, the disposal of such proceedings of sentence of any court.

The grounds for processing sensitive PII include:

- explicit consent of the individual;
- performance of employment law obligations;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or in order to exercise legal rights; or
- processing for medical purposes.

The DPA does not impose any sector-specific rules.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

Data owners are obliged to notify individuals of:

- the data owner's identity;
- its nominated representative in the UK (if applicable);
- the purposes for which the PII will be processed; and
- any further information required to make the processing fair.

Examples of such further information are unexpected uses of the PII, third-party disclosures and transfers to third countries not offering adequate protection.

Where the PII is collected directly from the individual, notice is required 'so far as practicable' and must be provided at the time of collection. Where the PII is obtained from another source, notice must be provided at the time of (or as soon as practicable thereafter) the data owner first processing the PII, or disclosure to a third party being envisaged.

13 Exemption from notification

When is notice not required?

Where PII is obtained from a third party and is required for a statutory purpose, or the provision of notice would involve disproportionate effort, notice is not required as long as the individual has not previously signified in writing that he or she requires a notice. A PII owner that relies upon this provision relating to disproportionate effort must keep a record of the fact.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals have rights of access, amendment and objection. A data owner must provide the individual with a copy of the PII it holds on him or her upon request. Individuals may request amendment of inaccurate data, and may object to processing where it is likely to cause substantial unwarranted damage or distress. Further, individuals may object at any time to the processing of their PII for the purposes of direct marketing.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The data owner must ensure that PII is relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The data owner must ensure that PII is adequate, relevant and not excessive in relation to the purpose for which it is held. This means that the data owner should not collect or process unnecessary or irrelevant PII. The DPA does not impose any specified retention periods. PII may only be held as long as is necessary for the purposes for which it is processed.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII may only be used for specified and lawful purposes, and may not be processed in any manner incompatible with those purposes. The purposes may be specified in the notice given to the individual or the registration lodged with the ICO.

In addition, recent case law has confirmed the existence of a tort of 'misuse of private information'. Under this doctrine, the use of private information about an individual for purposes to which the individual has not consented may give rise to a separate action in tort against the data owner, independent of any action taken under the DPA.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

PII may not be processed for new purposes unless the further purposes are lawful (ie, based on a lawful ground; see question 10). It may be processed for a new purpose as long as that purpose is not incompatible with the original purpose, but notice of the new purpose must be provided to the individual. Where a new purpose would be incompatible with the original purpose, it must be legitimised by the consent of the individual unless an exemption (non-disclosure exemption) applies. For example, PII may be further processed for certain specified public interest purposes, including the prevention of crime or prosecution of offenders and processing for research, historical or statistical purposes.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

The DPA does not specify the types of security measures that data owners must take in relation to PII. Instead, the DPA states that data owners must have in place 'appropriate technical and organisational measures' to protect against 'unauthorised or unlawful processing of [PII] and against accidental loss or destruction of, or damage to, [PII]'.

Under the relevant provisions, in assessing what is 'appropriate' in each case, data owners should consider the nature of the PII in question and the harm that might result from its improper use, or from its accidental loss or destruction. The data owner must take reasonable steps to ensure the reliability of its employees.

Where a data owner uses an outsourced provider of services to process PII it must chose a processor providing sufficient guarantees of security, take reasonable steps to ensure that these are delivered, require the processor to enter into a contract in writing or evidenced in writing under which the processor will act only on the instructions of the owner and apply equivalent security safeguards to those imposed on the data owner.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

There is no obligation in the DPA on data owners to report data breaches either to the ICO or to the affected individuals; however, government departments have been instructed to report breaches and the ICO has issued 'best practice' guidance, advising other data owners to determine whether a breach is sufficiently serious to warrant reporting based on a range of factors, including the number of individuals affected, the nature of the data and whether the breach was malicious in nature. The ICO does not expect every breach to be reported, and small breaches should be dealt with by the relevant data owner. Providers of electronic communication services are obliged to report some types of breach.

In most circumstances, a data processor that suffers a data breach would be expected (under the terms of a well-drafted data processing agreement) to notify the data owner of that breach. The data owner then would decide, in accordance with the principles set out above, whether to report that breach.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is no legal requirement to appoint a person to the role of 'data protection officer', but many organisations do appoint such officers. The role will generally cover, at a minimum, the maintenance of the organisation's registration and the handling of enquiries and requests from individuals.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Where a data owner takes advantage of an exemption from the obligation to register its data processing with the ICO, it may be obliged to provide an enquirer with a written statement describing the processing being carried out. A record must be kept of any decision to rely on the provision in relation to disproportionate effort as described in question 13. There are no other specific obligations to retain internal records or maintain internal processes; however, the DPA requires that PII shall be 'adequate, relevant and not excessive', and 'shall be accurate and, where necessary, kept up to date'. Data owners may need to maintain internal records and establish internal processes or documentation to satisfy these requirements in practice. In addition, where a data owner makes a decision that may later be queried by an individual or the ICO, it is advisable for the data owner to keep clear records of that decision and the reasons for it. For example, where a data owner makes its own adequacy determination for the purposes of data transfers (see question 31) it should keep a record of that determination and the information that gave rise to it.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

Data owners are required to register with the ICO, but several exceptions exist. There is no obligation to register if any of the following applies:

- no processing is carried out on a computer (or other automated equipment);
- the processing is performed solely for the maintenance of a public register;
- the data owner is a not-for-profit organisation, and the processing is only for the purposes of establishing or maintaining membership or support of that organisation; or
- the data owner only processes PII for one or more of these purposes:
  - staff administration;
  - advertising, marketing and public relations; or
  - accounts and records.

An entity that is a data processor only (and not a data owner) is not required to register.

24 Formalities

What are the formalities for registration?

There is a two-tier registration fee structure. The higher-tier fee, currently set at £500, applies to data owners that either:

- have a turnover of £25.9 million and at least 250 members of staff; or
- are a public authority with at least 250 members of staff.

All other data owners (including all registered charities and small occupational pension schemes) fall into in the lower-tier category, paying £35, unless they are exempt. The registration period is one year, and the registration expires at the end of that period unless it is renewed.

The data owner must include in the registration application its name, address, and a description of the relevant processing, the purposes of that processing, details of third-party recipients of the relevant PII and information about transfers outside the UK, as well as a general description of the security measures it has in place. Once registered, a data owner is responsible for ensuring that the registration details are kept up to date.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

PII must not be processed unless the data owner is currently registered with the ICO and, once registered, keeps its registration details up to date.

If the data owner is not registered or fails to maintain an accurate entry in the register, the data owner is guilty of a criminal offence that could lead to a fine of up to £5,000 in a magistrate's court, or unlimited fines in a crown court. As previously noted, an entity that is a data processor only (and not a data owner) is not required to register.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The ICO has no power to refuse an application for registration provided that it is made in the prescribed form and includes the applicable fee. An entry that contains inaccurate content or statements may be rejected by the ICO as an invalid application, but there is no power to refuse a valid application.

27 Public access

Is the register publicly available? How can it be accessed?

The register is publicly available, free of charge, from the ICO's website (https://ico.org.uk/esdwebpages/search).

A copy of the register on DVD may also be requested, by sending an e-mail to accessICOinformation@ico.org.uk.

28 Effect of registration

Does an entry on the register have any specific legal effect?

An entry on the register does not cause the data owner to be subject to obligations or liabilities that it would not otherwise be subject to.

The data owner's entry on the register must specify the purposes for which the PII will be processed. If those purposes change, the data owner must update the information on the register (there is no fee for updating the register).

There is no obligation to give notice to individuals in connection with the registration of the data owner.

The contents of the entry have the effect of specifying the purposes of the processing, but notice must also be provided to individuals of the processing.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Entities that provide outsourced processing services are 'data processors' under the DPA. Data processors do not have direct legal obligations under the DPA in respect of the PII that they process as outsourced service providers. The obligation to ensure that the processor processes PII in accordance with the DPA rests with the data owner. The data owner must ensure that each processor it selects offers sufficient guarantees that the relevant PII will be held with appropriate security, and takes steps to ensure that these guarantees are fulfilled. The data owner must also enter into a contract in writing with the processor under which the processor must be bound to act only on the instructions of the data owner and to apply security controls and standards that meet those required by the DPA.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

It is a criminal offence to knowingly or recklessly obtain or disclose PII without the consent of the data owner or procure the disclosure of PII to another party without the consent of the data owner. This prohibition is subject to a number of exceptions, such as where the action was taken for the purposes of preventing or detecting crime. The staff of the ICO are prohibited from the disclosure of PII obtained in the course of their functions other than in accord with those functions.

There are no other specific restrictions on disclosure of PII, other than compliance with the general principles described earlier, and the cross-border restrictions as set out below.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII outside the EEA is prohibited unless that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals in relation to the processing of their PII.

Data owners in the UK are entitled to make their own determination of adequacy in relation to a jurisdiction to which PII will be transferred. In assessing the adequacy of such a jurisdiction, the data owner should take into account a variety of factors, including the nature of the PII, the law in force in the country of destination, and security measures taken in relation to the data and the purposes of the processing.

Transfers are permitted where:

- the European Commission (Commission) has made a finding in relation to the adequacy of the country or territory;
- the Commission has made a finding in relation to the relevant transfers; or
- one or more of the derogations applies.

The derogations include:

- where the data owner has the individual's consent to the transfer;
- the transfer is necessary for a contract with the data subject;
- the transfer is necessary for legal proceedings;
- the transfer is necessary to protect the vital interest of the individual; and
- the terms of the transfer have been approved by the ICO.

Commission findings have been made in respect of the use of approved standard form model clauses for the export of PII and the adoption of a self-regulatory scheme in the US called 'Safe Harbor'. In addition, entities within a single corporate group can enter into data transfer agreements known as 'Binding Corporate Rules', which must be approved by the supervisory authorities in the relevant EU member states.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

Transfer requires no specific notification to the ICO and no authorisation from the ICO. A description of overseas transfers must be included on the register (see question 24).

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on transfer apply equally to transfers to data processors and data owners.

Onward transfers are taken into account in assessing whether adequate protection is provided in the receiving country. Onward transfers are covered in the Commission-approved model clauses and the Safe Harbor approval.

Onward transfers are not controlled specifically where a transfer is made to a country that has been the subject of an adequacy finding by the Commission. It would be anticipated that the law of the recipient country would deal with the legitimacy of the onward transfer.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Individuals have the right to request access to PII that relates to them. A request must be in writing and a small fee is payable. Within 40 days of receipt of a valid request the data owner must supply a statement that it processes or does not process PII relating to that subject and, if it does so, a description of the PII, the purposes of the processing and recipients of the

PII, together with a copy of the PII in an intelligible form and any information available to the owner as to the sources of the PII.

A data owner must be satisfied as to the identity of the individual making the request. A data owner does not have to provide third-party data where that would breach the privacy of the third party and may reject repeated identical requests.

In some cases the data owner may withhold PII to protect the individual, for example where health data are involved, or to protect other important specified public interests such as the prevention of crime. All such exceptions are specifically delineated in the law.

35 Other rights

Do individuals have other substantive rights?

Individuals have the following further rights:

- to object to the processing of PII for the purposes of direct marketing;
- to object to the processing of PII that would cause substantial unwarranted damage or distress;
- to restrict the taking of automated decisions in a limited number of cases; and
- to seek rectification or erasure or blocking of PII where the data are inaccurate.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to receive compensation if the individual suffers damage as a result of the contravention of the DPA by a data owner. Where an individual is entitled to compensation for damage they may also seek compensation for any associated distress. In the absence of pecuniary damage, the DPA indicates that mere distress or injury to feelings is not a basis for compensation. However, recent case law has clarified that damages for distress or injury to feelings may be granted in some cases. Where the contravention relates to the purposes of journalism or the production of literary or artistic works, compensation may be awarded for distress alone.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals may take action in the courts to enforce any of the rights described in questions 34–36.

The ICO has no power to order the payment of compensation to individuals. Therefore, an individual who seeks compensation must take an action to the courts. All the other rights of individuals can be enforced by the ICO using the powers described in question 2.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The DPA provides three types of exemptions: exemptions from the obligations that limit the disclosure of PII; exemptions from the obligations to provide notice of uses of PII; and exemptions from the rights of access.

The grounds for exemption include exemptions to protect freedom of expression, to protect national security and policing, to support legal privilege, to protect the actions of regulatory authorities, and to protect the collection of taxes and the position of the armed forces.

Exemptions also apply to protect individuals who may be vulnerable, such as those who are suffering from mental illness.

Further exemptions apply where the PII is made publicly available under other provisions.

As noted in question 23, some forms of processing of PII are exempt from the obligation to register the processing on the public register.

Specific exemptions apply to allow the retention and use of PII for the purposes of research.

All exemptions are limited in scope and most apply only on a case-by-case basis.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

Data owners may appeal orders of the ICO to the General Regulatory Chamber (First-tier Tribunal). Appeals must be made within 28 days of the ICO notice and must state the full reasons and grounds for the appeal (ie, that the order is not in accordance with the law, or the ICO should have exercised its discretion differently).

Appeals against decisions of the General Regulatory Chamber (First-tier Tribunal) can be made (on points of law only) to the Administrative Appeals Chamber of the Upper Tribunal, appeals from which may be made to the Court of Appeal.

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

It is unlawful to store information (such as a cookie) on a user's device, or gain access to such information, unless the user is provided with clear and comprehensive information about the storage of, and access to, that information, and has provided consent. Such consent is not, however, required where the information is:

HUNTON& WILLIAMS

Rosemary P Jay **rjay@hunton.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.hunton.com

- only used for transmission of communications over electronic communications networks; or
- strictly necessary for the provision of a service requested by the user.

The ICO has recognised that in some circumstances, it may be impractical to obtain consent before a cookie is placed and subsequent validation may be the only option.

41 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

It is unlawful to send unsolicited electronic marketing (ie, via technologies such as SMS, fax or e-mail) unless the consent of the recipient has been obtained. However, an unsolicited marketing e-mail may be sent to a recipient whose contact details were obtained in the course of a sale, or negotiation of sale, of a product or service, provided that the unsolicited marketing relates to similar products or services, the recipient is given a simple and free of charge means to opt out of receiving such marketing and has not yet opted out.

It is generally permissible to make unsolicited telephone marketing calls, unless: the recipient has previously notified the caller that he or she does not wish to receive such calls; or the recipient's phone number is listed on the directory of subscribers who do not wish to receive such calls. Any individuals may apply to have their telephone number listed in this directory; a separate provision covers corporate entities.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law