ICLG

The International Comparative Legal Guide to:

Data Protection 2014

1st Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

BANNING
Barrera, Siqueiros y Torres Landa, S.C.
CMS Reich-Rohrwig Hainz
Dittmar & Indrenius
DLA Piper
ECIJA ABOGADOS
Eversheds
Gilbert + Tobin Lawyers
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
KALO & ASSOCIATES
Koep & Partners
Marrugo Rivera & Asociados, Estudio Jurídico
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Raja, Darryl & Loh
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Account Managers
Edmond Atta, Beth Bassett, Antony Dine, Susan Glinska, Dror Levy, Maria Lopez, Florjan Osmani, Paul Regan, Gordon Sambrooks, Oliver Smith, Rory Smith

Sales Support Manager
Toni Wyatt

Sub Editors
Nicholas Catlin
Amy Hirst

Editors
Beatriz Arroyo
Gemma Bridge

Senior Editor
Suzie Kidd

Global Head of Sales
Simon Lemos

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.
May 2014

ISBN 978-1-908070-98-2
ISSN 2054-3786

Strategic Partners

General Chapter:

Country Question and Answer Chapters:

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

EDITORIAL

Welcome to the first edition of *The International Comparative Legal Guide to: Data Protection*.

This guide provides the international practitioner and in-house counsel with a comprehensive worldwide legal analysis of the laws and regulations of data protection.

It is divided into two main sections:

One general chapter entitled *Data Protection – a Key Business Risk*.

Country question and answer chapters. These provide a broad overview of common issues in data protection laws and regulations in 29 jurisdictions.

All chapters are written by leading data protection lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editor Bridget Treacy of Hunton & Williams for her invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.co.uk.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

Chapter 14

Ireland

John O'Connor

Matheson

Anne-Marie Bohan

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Data Protection Acts 1988 and 2003 ("DPA").

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

S.I. No. 658/2007 – Data Protection (Fees) Regulations 2007

This outlines the fee for registration and for prior checking.

S.I. No. 347/1988 – Data Protection (Fees) Regulations, 1988

The fee that an organisation may charge for an Access Request (€6.35) and the fee for a certified copy of a Register entry (€2.54).

S.I. No. 657/2007 – Data Protection Act 1988 (Section 16(1)) Regulations 2007

This outlines the organisations that will be required to register with the ODPC.

S.I. No. 351/1988 – Data Protection (Registration) Regulations, 1988

This outlines the details that must be contained in forms for registration with the ODPC.

S.I. 350 of 1988 – Period of Registration

This outlines the period that registration lasts for (1 year).

S.I. No. 83/1989 – Data Protection (Access Modification) (Social Work) Regulations, 1989

Outlines specific restrictions in respect of social work data.

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

S.I. No. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ("E-Privacy Regulations")

This deals with specific data protection issues relating to use of electronic communication devices, and particularly with direct marketing restrictions.

S.I. No. 95/1993 – Data Protection Act, 1988 (Section 5 (1) (D)) (Specification) Regulations, 1993

This outlines the exemption from the DPA of the use of personal data in the performance of certain functions of the Central Bank, the National Consumer Agency, various functions performed by auditors under the Companies Acts, etc.

S.I. No 421 of 2009 – Data Protection Act 1988 (Section 5(1)(D)) (Specification) Regulations 2009

This outlines the exemption from the DPA of the use of personal data in the performance of certain functions of the Director of Corporate Enforcement and inspectors appointed by the High Court or Director of Corporate Enforcement.

S.I. No. 687/2007 – Data Protection (Processing of Genetic Data) Regulations 2007

This outlines restrictions in respect of processing genetic data in relation to employment.

S.I. No. 81/1989 – Data Protection Act, 1988 (Restriction of Section 4) Regulations, 1989

This outlines the restriction on the right of access to information on adopted children and information the Public Service Ombudsman gets during an investigation.

S.I. No. 82/1989 – Data Protection (Access Modification) (Health) Regulations, 1989

This outlines certain restrictions in the right of access relating to health data.

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

The Office of the Data Protection Commissioner ("ODPC").

2 Definitions

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

- **"Personal Data"**

  Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

- **"Sensitive Personal Data"**

  Means personal data as to:

  (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;

  (b) whether the data subject is a member of a trade union;

  (c) the physical or mental health or condition or sexual life of the data subject;

  (d) the commission or alleged commission of any offence by the data subject; or

(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

- **"Processing"**

In relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

(a) obtaining, recording or keeping the information or data;

(b) collecting, organising, storing, altering or adapting the information or data;

(c) retrieving, consulting or using the information or data;

(d) disclosing the information or data by transmitting, disseminating or otherwise making it available; or

(e) aligning, combining, blocking, erasing or destroying the information or data.

- **"Data Controller"**

Means a person who, either alone or with others, controls the contents and use of personal data.

- **"Data Processor"**

Means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

- **"Data Owner"**

No definition in Irish law.

- **"Data Subject"**

Means an individual who is the subject of personal data.

- **"Pseudonymous Data"**

No definition in Irish law.

- **"Direct Personal Data"**

No definition in Irish law.

- **"Indirect Personal Data"**

No definition in Irish law.

3 Key Principles

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

- **Transparency**

Data subjects must be provided with information relating to the processing of their data. This includes:

a) the identity of the data controller or their representative and/or the data processor;

b) the purposes for which the data are intended to be processed; and

c) any other information that is necessary, having regard to the specific circumstances in which data are to be processed, including but not limited to details of recipients or categories of recipients of the personal data and information as to the existence of the right of access and the right to rectify data.

- **Lawful basis for processing**

(a) consent of the data subject (specific, freely given, informed); and

(b) the processing is necessary:

i) for the performance of a contract to which the data subject is a party;

ii) in order to take steps at the request of the data subject prior to entering into a contract;

iii) for compliance with a legal obligation to which the data controller is subject rather than an obligation imposed by contract;

iv) to prevent:

I) injury or other damage to the health of the data subject; and

II) serious loss or damage to property of the data subject, or otherwise to protect his or her vital interests where the seeking of the consent of the data subject is likely to result in those interests being damaged;

v) for compliance with a legal obligation including:

I) the administration of justice;

II) for the performance of a function conferred on a person by law;

III) for the performance of a function of the government or a minister of the government;

IV) for the performance of any other function of a public nature which is performed in the public interest; and

vi) for the purposes of the legitimate interests pursued by the data controller (or third party to whom the personal data are disclosed).

- **Purpose limitation**

Personal data should only be obtained for one or more specified, explicit and legitimate purposes and should not be further processed in a manner incompatible with that power or those purposes.

- **Data minimisation**

Personal data should not be kept for longer than is necessary for the purposes for which they were obtained.

- **Proportionality**

Personal data collected must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or are further processed.

- **Retention**

Personal data should not be kept for longer than is necessary for the purpose for which it was obtained.

If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

- **Other key principles**

Data security (covered in more detail in section 13 below).

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**

Under section 3 of the DPA, data subjects have the right to, free of charge, find out if an organisation or an individual holds information about them. This includes the right to be given a description of the information and to be told the purposes for which that information is held. A request for this information must be made in writing by the data subject and the individual must receive a reply within 21 days according to the DPA.

Section 4 of the DPA provides that data subjects have the right to obtain a copy of any information which relates to them that is held either on a computer or in a structured manual filing system, or that is intended for such a system. A fee of €6.35 is required when a request is made under

section 4 and the organisation or entity is given 40 days to reply to such a request.

Exceptions to the right of access:

The DPA set out specific circumstances when an individual's right of access to their personal information held by an organisation may be restricted.

Disclosure is not required if the information would be likely to:

a) hinder the purposes of anti-fraud functions;

b) damage international relations;

c) impair the security or order in a prison or detention facility;

d) hinder the assessment or collection of any taxes or duties; or if

e) disclosure of estimates of damages or compensation regarding a claim against the data controller is likely to cause damage to the data controller.

Certain information is also exempt from disclosure if the information is:

a) protected by legal privilege;

b) used for historical, statistical or research purposes, where the information is not disclosed to anyone else, and where the results of such work are not made available in a form that identifies any of the individuals involved;

c) an opinion given in confidence; or

d) used to prevent, detect or investigate offences, or will be used in the apprehension or prosecution of offenders.

If a request would be either disproportionately difficult or impossible to process the data controller or processer does not have to fulfil the request.

Exemptions also apply in respect of access to social work data, disclosure of such may be refused if it is likely to cause serious damage to the physical, mental or emotional condition of the data subject.

A request for health data may also be refused if disclosure of the information is likely to seriously damage the physical or mental health of that data subject.

- **Correction and deletion**

Section 6 of the DPA provides data subjects with the right to request in writing to have their data either deleted or corrected where the data is not obtained lawfully or is inaccurate. The data controller or processor must respond within a reasonable amount of time and no later than 40 days after the request. There is no express right of a data subject to request the deletion of their information if it is being processed lawfully.

- **Objection to processing**

Under Section 6A of the DPA, data subjects have the right to object to processing which is likely to cause damage or distress. This right applies to processing that is necessary for the purposes of legitimate interests pursued by the data controller to whom the personal data is, or will be disclosed or processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

- **Objection to marketing**

Under section 2.7 of the DPA, data subjects have the right to, following a request by writing, require the data controller to cease processing data for that purpose, and where it is only retained for that purpose they have the right to have it erased. The data controller must do this within 40 days.

Under sections 13 and 14 of the E-Privacy Regulations, data subjects have the right to have their "opt-out" preference recorded in the National Directory Database, which constitutes an objection to direct marketing to them.

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

Under Section 10 of the DPA, data subjects have a right of complaint to the ODPC in relation to the treatment of their personal data. The ODPC must investigate such complaints unless it considers them to be 'frivolous or vexatious'.

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.)

Generally, all data controllers and processors must register unless an exemption applies, either under Section 16(1)(a) or (b) or under SI No. 657 of 2007. Under section 3 of SI No. 657 of 2007 the following are excluded from registration:

a) organisations that only carry out processing to keep, in accordance with law, a register that is intended to provide information to the public;

b) organisations that only process manual data (unless the personal data had been prescribed by the ODPC as requiring registration); and

c) organisations that are not established or conducted for profit and that are processing personal data related to their members and supporters and their activities.

There is also a wide exemption applied to normal commercial activity, which by definition requires the processing of personal data.

If an exemption does apply however, it is limited only to the extent to which personal data is processed within the scope of that exemption.

Additionally, the Irish Minister for Justice and Equality has specified that the following data controllers and data processors are not required to register (provided they do not fall within any of the above categories):

a) data controllers who only process employee data in the ordinary course of personnel administration and where the personal data is not processed other than where it is necessary to carry out such processing;

b) solicitors and barristers;

c) candidates for political office and elected representatives;

d) schools, colleges, universities and similar educational institutions;

e) data controllers (other than health professionals who process data relating to the physical or mental health of a data subject for medical purposes) who process data relating to past, existing or prospective customers or suppliers for the purposes of:

f) advertising or marketing the data controller's business, activity, goods or services;

g) keeping accounts relating to any business or other activity carried on by the data controller;

h) deciding whether to accept any person as a customer or supplier;

i) keeping records of purchases, sales or other transactions for the purpose of ensuring that requisite payments and deliveries are made or services provided by or to the data controller in respect of those transactions;

j) making financial or management forecasts to assist in the conduct of business or other activity carried on by the data controller;

k) performing a contract with the data subject;

l) where the personal data is not processed other than where it is necessary to carry out such processing for any of the purposes set out above;

m) companies who process personal data relating to past or existing shareholders, directors or other officers of a company for the purpose of compliance with the Companies Acts;

n) data controllers who process personal data with a view to the publication of journalistic, literary or artistic material; and

o) data controllers or data processors who operate under a data protection code of practice.

Subject to the above, all data controllers and data processors are required to register, except to the extent that:

a) they carry out processing for the sole purpose of keeping in accordance with law of a register that is intended to provide information to the public and is open to consultation either by the public in general or by any person demonstrating a legitimate interest;

b) they process manual data (other than such categories, if any, of such data as may be prescribed);

c) they carry out any combination of the above; or

d) the data controller is a body that is not established or conducted for profit and is carrying out processing for the purposes of establishing or maintaining membership of or support for the body or providing or administering activities for the members of the body or persons who have regular contact with the body.

The ODPC is obliged not to accept an application for registration from a data controller who keeps 'sensitive personal data' unless he or she is of the opinion that appropriate safeguards for the protection of the privacy of the data subjects concerned are being, and will continue to be, provided by him or her.

The DPA also provide that, where a data controller intends to keep personal data for two or more related purposes, they are only required to make one application in respect of those purposes. If, on the other hand, they intend to keep personal data for two or more unrelated purposes, then they will be required to make separate applications in respect of each of those purposes and entries will be made in the register in accordance with each such application.

Where the ODPC refuses an application for registration he shall notify the applicant in writing and specify the reasons for the refusal. An appeal against such decision can be made to the Circuit Court.

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 are made per legal entity.

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.)

Any legal entity processing personal data in Ireland not subject to the exemptions in question 5.1 above must register with the ODPC.

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.)

There are separate registration forms available on the ODPC's website for the registration of either a data processor or a data controller. A data controller must provide a general statement of the nature of their business or trade or profession and of any additional purposes for which they keep personal data. Each application of personal data relating to the purposes that the controller lists along with the types of personal data (such as name, email, date of birth, etc.) must also be listed or described. For each of these applications listed, a list of the persons or bodies to whom the personal data maybe disclosed must also be given.

For data processors, a name, address and details on the nature of the data being processed must also be provided.

Information on any sensitive personal data that is kept by the controller must also be given (such as data relating to race, religion, sexual life, criminal convictions, etc.).

If any transfers are made (or intended to be made) to a country outside of the EU Member States, a list of these countries along with a description of the data to be transferred and the purpose of the transfer must be provided.

Finally, for both processors and controllers details of a 'compliance person' who will supervise the application of the DPA within the organisation in relation to personal data which is collected must be given.

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

a) Fines:
   i) maximum €3,000 on summary conviction; and
   ii) maximum €100,000 on indictment; and

b) order for erasure of personal data.

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

	Postal Applications	Online Applications
Applicants with 26 Employees or more (inclusive)	€480	€430
Applicants with 6 to 25 Employees (inclusive)	€100	€90
Applicants with 0 to 5 Employees (inclusive)	€40	€35

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

Registration must be renewed annually.

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

Prior approval required for transfer abroad in certain circumstances – see question 8.3 below.

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

See question 8.3 below.

6 Appointment of a Data Protection Officer

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

The appointment of a data protection officer is optional, though when registering with the Data Protection Commissioner both data controllers and processors must give details of a 'compliance person' who will act as a contact point for the ODPC.

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

As there is no legal requirement, there are no sanctions.

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

The advantages of voluntarily appointing a data protection officer include:

a) ensuring an officer with appropriate qualifications and data protection expertise within an organisation;

b) helps establish central professional data protection management within the organisation, particularly risk management functions, with one contact point for all data protection related issues;

c) builds a relationship with the ODPC;

d) develops relationships with customers and a reputation generally;

e) helps handle emergencies, such as audits or data breaches; and

f) improves data protection awareness within the organisation.

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

As there is no legal requirement for a data protection officer, no specific qualifications are required.

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

In practice, it is the duty of data protection officers to ensure that the organisation complies with the DPA and to be the contact point relating to all such matters. They provide support, assistance, advice and training to all employees of an organisation on data protection matters and add to any risk management process.

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

As there is no legal requirement for a data protection officer, there is no need to notify this to the ODPC.

7 Marketing and Cookies

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

When using automatic dialling machines, fax, email or SMS to send messages to an individual or making telephone calls to an individual or non-natural person's mobile telephone to make direct marketing communications, the data subject's prior opt-in consent must be obtained.

The use of automatic dialling machines, fax, email or SMS for direct marketing to a non-natural person (i.e. body corporate) is allowed as long as they have not either recorded their objection in the National Directory Database (under "objection to marketing" under question 4.1 above), or has not opted out.

Marketing messages may be sent by post to either an individual or non-natural person, unless they opt-out in writing.

The making of telephone calls for direct marketing to a subscriber or user is prohibited if the subscriber or user has recorded its objection in the National Directory Database (as under "objection to marketing" under question 4.1 above), or has opted out.

Where making direct marketing communication, the name, address and telephone number of the marketer must be included in the communication in order to give the data subject the option of opting-out.

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

Yes. The Data Protection Commissioner has pursued a number of prosecutions in recent years for offenders.

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

On summary conviction a fine of €5,000, or on indictment a €250,000 fine where it is a body corporate or in the case of a natural person, a fine of €50,000. A court may make an order for the destruction or forfeiture of any data connected with the breach.

Where the communication is done by post, a fine of €3,000 on summary conviction or €100,000 on indictment.

7.4 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 are not strictly necessary for a transaction that the data subject has requested require express and informed consent. This may be obtained as part of a prominent notification on a website containing a link to a cookie statement.

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

Where a cookie is strictly necessary to facilitate a transaction, (and that transaction has been specifically requested by the data subject), implied consent is acceptable.

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

The ODPC has been active in this field. For instance, in 2012, they wrote to 80 website operators seeking information on their consent procedures.

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

A fine of €5,000 and an order for the destruction or forfeiture of any data connected with the breach.

8 Restrictions on International Data Transfers

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

There is no restriction on the transfer of personal data to countries within the EEA. However, personal data may not be transferred outside the EEA unless one of the following applies:

a) the transfer is authorised by law;

b) consent to the transfer is given by the data subject;

c) the transfer is necessary for the performance of a contract to which the data subject is party;

d) the transfer is necessary to conclude a contract with someone other than the data subject, where it is in their interests;

e) the transfer is necessary for reasons of substantial public interest;

f) the transfer is necessary for obtaining legal advice for legal proceedings;

g) the transfer is necessary to prevent injury or damage to the data subject;

h) the personal data to be transferred are an extract from a statutory public register established by law for public consultation; or

i) the transfer is done through one of the mechanisms described in question 8.2 below.

Even where one of the above elements exists, the Data Protection Commissioner retains the power to prohibit the transfer of personal data abroad to any country inside or outside the EEA.

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

In addition to the methods outlined above, the three methods by which companies typically transfer personal data abroad are as follows:

a) Use of "model clauses" between the data controller and the person/organisation to whom they intend to pass the information to abroad. These are contractual clauses approved by the EU Commission and which assure an adequate level of protection for the personal data. They do not usually require the approval of the ODPC, however it can approve transfers based on contractual clauses which do not directly conform to the European model clauses.

b) Transfer to a country that is on the EU Commission "adequate standard of protection" list, or US organisations that have agreed to be bound by the rules of the "Safe Harbour" agreement (essentially a streamlined version of EU data protection law).

c) A further method that is rarely used is the use of Binding Corporate Rules ("BCR"), whereby personal data can be transferred to other companies within a group and based abroad, as long as certain legally enforceable rules exist within the group whereby they must give the data an adequate level of protection. It is rarely used because of the expense and difficulty involved in having these rules approved by the Data Protection Commissioner.

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.

Where data is transferred abroad under contracts that vary from the "model clauses", this must be notified to and approved by the ODPC by application to them. There is no necessity to deposit the contracts with the ODPC once the process is complete. Ordinarily, the ODPC will only consider authorising contracts that are general in nature, i.e., 'model contracts' that can be relied upon by a number of different data controllers within a sector or category rather than specific contracts. The time this process takes varies depending on the nature of the modifications to the model clauses.

The ODPC must also approve BCR mechanisms used to transfer data abroad but within a corporate group. This requires engagement with the ODPC by the company involved. At the time of writing, only one company within Ireland has implemented BCRS, as they are difficult to obtain. This took almost a year of engagement with the ODPC.

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.)

Ireland does not have specific whistleblowing legislation, so it is a matter for each employer to decide who may make reports and about whom such reports can be made. However, there should be no discriminatory element in the scope decided by the employer. For instance, if it is open to employees, it should be open to all classes of employees, be they part-time workers, fixed-term workers or agency workers.

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?

Anonymous reporting is discouraged under non-binding guidance from the Data Protection Commissioner.

In our experience, companies deal with this by pointing out to whistleblowers the benefits in their whistleblowing policy of disclosing their identity, such as protection from retaliation and the increased effectiveness of any whistleblowing report where identity is given. They also demonstrate that the identity of whistleblowers is kept confidential. However, companies generally do not make it mandatory for identity to be disclosed in order for a report to be acted on.

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.

There is no requirement to register whistleblower hotlines in Ireland.

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)?

There is no requirement to register separately for the use of CCTV.

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

There is no hard restriction on the type of monitoring that employees may be put under including monitoring of their electronic communications or surveillance by CCTV. However, as this involves the collection of personal data, the principles outlined in question 3.1 above must be followed, in particular the principle of proportionality, whereby employers must only collect relevant, adequate and non-excessive amounts of personal data, having regard to their legitimate aims.

The circumstances in which different types of personal data may be collected are a matter of degree, involving a balance between legitimate aims of the employer. For instance, the constant monitoring of employees by CCTV would be difficult to justify, unless there was a specific security need for it.

Employees have a legitimate right to privacy in relation to communications made from the workplace unless informed otherwise, so there is an additional requirement that they give their consent to monitoring, as outlined in question 10.3 below.

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

Employees must be notified of the existence of the surveillance and also the purposes for which the data are processed. Surveillance of electronic communications and otherwise is generally notified by making the employee aware of an acceptable usage policy.

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

The extent to which a works council/trade union/employee representative needs to be notified of such surveillance will depend on (i) the scope of the agreement with the relevant body, (ii) whether this topic has already been covered in the contract of employment, and (iii) the likelihood that the employer will need to rely on the monitoring in the future (in order to provide evidence in defending a claim from an employee, for example).

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

There is no requirement to make a separate registration, notification or prior approval with the ODPC in respect of employee monitoring.

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)?

Personal data may be processed in the cloud, subject to the DPA.

Under non-binding guidance from the ODPC, the data controller must ensure that the processor (the cloud provider) has sufficient security precautions in place for the personal data, which is a requirement placed on the data controller as outlined in question 13.1 below. The cloud should be able to give assurances on:

a) continued access to data by the data controller (backup and recovery measures);

b) prevention of authorised access to data (covers both protection against external "hacking" attacks and access by the cloud provider's personnel or by other users of the datacentre);

c) adequate oversight including by means of contract of any sub-processors used;

d) procedures in the event of a data breach (so that the data controller can take necessary measures); and

e) right to remove or transfer data (if the data controller wishes either to move the data back under its own direct control or move it to another cloud provider).

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 must be a written contract with the cloud provider and any sub-processors. The obligations imposed by it should include:

a) the cloud providers and sub-processors will only process data as instructed by the data controller;

b) the security requirements as outlined in question 11.1 above; and

c) model contract clauses where the data is processed outside the EEA.

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)?

There is nothing in Irish law that specifically prevents the use of big data and analytics, and no specific laws or binding guidance covering the precise due diligence required.

However, as data protection issues are likely to arise in many projects, it is strongly recommended to undertake thorough due diligence.

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)?

Under section 2 of the DPA, data controllers must have "appropriate security measures" in place, taking into account:

a) the state of technological development;

b) the cost of implementing the measures;

c) the harm that might result; and

d) the nature of the data concerned.

These measures must be appropriate to the nature of the data concerned and must provide a level of security that is appropriate to the potential level of harm that could result from any unauthorised or unlawful processing or from any loss or destruction of personal data. Data controllers and processors must also ensure that their employees comply with any and all security measures in place.

Non-binding guidance from the ODPC provides guidance on access control, access authorisation, encryption, anti-virus software, firewalls, software patching, remote access, etc.

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.

Providers of publicly available electronic communications services or public communications networks in Ireland are subject to a mandatory reporting obligation under the E-Privacy Regulations. For entities that are not providers of such networks or services, there is no strict legal requirement under the DPA to report data breaches. However, the ODPC expects voluntary breach reporting as outlined in the 'Personal Data Security Breach Code of Practice' ("the Code"), which contains specific data security breach guidelines.

The Code is non-binding in nature, although certain industries have developed codes of practice (for example, the insurance industry) which make the Code binding on industry stakeholders on a voluntary basis.

Under the Code, any incident which has put personal data at risk should be reported to the ODPC as soon as the data controller becomes aware of it. There are some limited exceptions to this provided for in the Code i.e., this is not required where:

a) it affects fewer than 100 data subjects;

b) the full facts of the incident have been reported without delay to those affected;

c) the breach does not involve sensitive personal data or personal data of a financial nature; or

d) if the personal data was protected by technological measures (such as encryption) to such an extent that it would be unintelligible to any person who is not authorised to access it, then the data controller may decide that there is no risk to the personal data (and so no notification to the data subject is necessary).

If the data controller is unclear about whether to report the incident or not, the Code advises that the incident should be reported to the ODPC. The Code advises that the controller should make contact with the ODPC within two working days of the incident occurring.

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 legal requirement, however the Code requires that data controllers must give immediate consideration to notifying the affected data subjects, unless there is no risk to the personal data because of a level of encryption as outlined in question 13.2 above.

The notification should include information on the nature of the personal data breach and a contact point where more information can be obtained and should also recommend measures to mitigate the possible adverse effects of the breach.

14 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigation of complaint under s.10 DPA, or of its own accord	Damages under negligence	Summary €3,000 Indictment €100,000
Privacy audit	This is not applicable	Summary €3,000 Indictment €100,000
Power to obtain information	This is not applicable	Summary €3,000 Indictment €100,000
Power to enforce compliance with DPA with enforcement notice	Damages under negligence	Summary €3,000 Indictment €100,000
Power of authorised officers to enter and examine premises	This is not applicable	Summary €3,000 Indictment €100,000

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

The ODPC exercises all of these powers on a regular basis.

The ODPC has conducted investigations recently, obtained information and conducted inspections of many organisations. A recent example of all three is the investigation, inspection and subsequent obtaining of information from LoyaltyBuild, a customer data database provider which had an extensive data breach.

The ODPC has also conducted many audits, and is currently running sequential audits of popular social media platforms including Twitter, LinkedIn and Facebook.

Finally, the ODPC has also used its power to enforce compliance with an enforcement notice on many occasions, including recently with the enforcement notice on a large telecoms provider, Eircom, to cease releasing personal data of subscribers.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

Where data are sought for use in civil proceedings in a foreign country, Irish companies may be compelled under a subpoena from an Irish court to provide them. This happens frequently between EU countries, but it is also possible for a request from outside the EU to succeed.

In relation to requests from foreign law enforcement agencies, there is a legal framework in place that allows for the law enforcement agencies of foreign signatories of certain Hague Conventions to seek the disclosure of data held by Irish companies by the Irish police, who then issue a warrant for it. Where the request is made by the law enforcement agencies of countries who are not signatories, this is determined by the Department of Justice and Equality on a case-by-case basis. Generally where proper undertakings are given by the agency making the request, it will be granted, and Irish companies will be compelled to disclose the data.

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

The ODPC has issued no guidance on E-discovery/disclosure to foreign law enforcement agencies.

John O'Connor

Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland

Tel: +353 1 232 2150
Fax: +353 1 232 3333
Email: john.oconnor@matheson.com
URL: www.matheson.com

John is a partner and head of the Technology and Commercial Contracts Group at Matheson. He has extensive experience in advising both suppliers and customers in relation to their commercial arrangements including their technology and outsourcing transactions.

On the technology side of John's practice, he advises his clients in relation to systems implementations, IT outsourcing and services arrangements, cloud computing, licensing and re-seller arrangements, data protection, intellectual property and e-business. On the commercial contracts side of John's practice he typically advises in relation to agency, distribution, franchising, manufacturing, business process outsourcing, facilities management and partnering agreements.

Prior to joining Matheson John worked at a leading London City firm where he gained significant experience of large scale technology and commercial transactions.

John is a frequent public speaker and regularly presents at seminars in relation to public procurement and in relation to outsourcing and managed services.

John has been published in legal and business journals in the UK and Ireland. John is a member of the Law Society of England and Wales (non-practising), a member of the Society for Computers and Law and a member of the UK National Outsourcing Association.

John co-authored the Irish chapters for Getting the Deal Through Life Sciences 2011 and PLC Outsourcing Handbook 2011/12.

Anne-Marie Bohan

Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland

Tel: +353 1 232 2212
Fax: +353 1 232 3333
Email: anne-marie.bohan@matheson.com
URL: www.matheson.com

Anne-Marie is a partner in both the Information Technology Law Group and the Asset Management and Investment Funds Group at Matheson, and is head of our Outsourcing Group. She advises on all aspects of outsourcing, information technology law and e-commerce law, with specific focus on the requirements of financial institutions and financial services providers in these areas.

Anne-Marie has extensive experience in drafting and negotiating contracts for the development, sale, purchase and licensing of hardware, software and IT systems for both suppliers and users of IT within the financial services industry and across a broad range of other industries. She has also acted in some of the largest value and most complex IT and telecommunications systems and services outsourcing contracts, including advising on the largest and highest value financial services outsourcing to date, in Ireland. Anne-Marie's practice also includes advising a broad range of clients on data protection and privacy issues, including employee data protection issues.

Anne-Marie has lectured on IT and financial services in the Law Society of Ireland and more broadly. She is author of the Ireland chapter in Outsourcing Contracts – a Practical Guide (Lewis, Third Ed, 2009) and in the forthcoming new edition and is co-author of the Irish chapter in PLC's Outsourcing Guide.

Matheson

Matheson's primary focus is on serving the Irish legal needs of international companies and financial institutions doing business in and through Ireland. Our clients include over half of the Fortune 100 companies. We also advise 7 of the top 10 global technology brands and over half of the world's 50 largest banks. We are headquartered in Dublin and also have offices in London, New York and Palo Alto. More than 600 people work across our four offices, including 75 partners and tax principals and over 350 legal and tax professionals.

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
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet

GLG
Global Legal Group

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