ICLG

The International Comparative Legal Guide to:

Data Protection 2017

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

Contributing Editors
Anita Bapat and Aaron P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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 2017

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Chapter 14

Ireland

Anne-Marie Bohan

Andreas Carney

Matheson

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation in Ireland is the Data Protection Act 1988, as amended by the Data Protection (Amendment) Act 2003 (together, the "**DPA**") which transpose, among others, European Directive 95/46/EC (the "**EU Data Protection Directive**") into Irish law.

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

The following legislation also impacts data protection:

- The Freedom of Information Act 2014, which provides a legal right for persons to access information held by a body to which FOI legislation applies, to have official information relating to himself/herself amended where it is incomplete, incorrect or misleading, and to obtain reasons for decisions affecting him/her.
- The Protected Disclosures Act 2014 (the "**Whistleblowers Act**"), which provides a general suite of employment protections and legal immunities to whistle-blowers who raise a concern regarding wrongdoings in the workplace and may be at risk of penalisation as a result.
- Criminal Justice (Mutual Assistance) Act 2008, Part 3, which enables Ireland to provide or seek various forms of mutual legal assistance to or from foreign law enforcement agencies.
- S.I. No. 337 of 2014 Data Protection Act 1988 (Commencement) Order 2014, which brought into force section 6(2)(b) and 10(7)(b) of the Data Protection Act 1988 and expands the notice requirements of a data controller.
- S.I. No. 338 of 2014 Data Protection (Amendment) Act 2003 (Commencement) Order 2014, which brought into force section 5(d) of the Data Protection (Amendment) Act, 2003 and makes it unlawful for employers to require employees or applicants for employment to make an access request, seeking copies of personal data, which is then made available to the employer or prospective employer. This provision also applies to any person who engages another person to provide a service.

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

The following sector-specific legislation impacts data protection:

- S.I. No. 81/1989 – Data Protection Act, 1988 (Restriction of Section 4) Regulations 1989, which restrict the right of access to information on adopted children and information which the Public Service Ombudsman acquires during an investigation.
- S.I. No. 82/1989 – Data Protection (Access Modification) (Health) Regulations 1989, which outline certain restrictions in the right of access relating to health data.
- S.I. No. 83/1989 – Data Protection (Access Modification) (Social Work) Regulations 1989, which outline specific restrictions in respect of social work data.
- S.I. No. 95/1993 – Data Protection Act 1988 (Section 5 (1)(D)) (Specification) Regulations 1993, which provide the exemption from the DPA in respect of the use of personal data in the performance of certain functions of the Central Bank of Ireland, the National Consumer Agency, various functions performed by auditors under the Companies Act 2014, etc.
- S.I. No. 687/2007 – Data Protection (Processing of Genetic Data) Regulations 2007, which outline restrictions in respect of processing genetic data in relation to employment.
- S.I. No. 421/2009 – Data Protection Act 1988 (Section 5(1)(D)) (Specification) Regulations 2009, which outline the exemption from the DPA in respect 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. 336/2011 – The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ("**E-Privacy Regulations**"), which implemented Directive 2002/58/EC, as amended by Directive 2006/24/EC and Directive 2009/136/EC, and deal with specific data protection issues relating to use of electronic communication devices, and particularly direct marketing restrictions.

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

The Office of the Data Protection Commissioner ("**ODPC**") is the data protection regulatory authority who is responsible for ensuring that individuals' data protection rights are respected. In 2014, Helen Dixon was appointed as the Data Protection Commissioner (the "**DPC**") by the Irish government, succeeding Billy Hawkes. The DPC is independent in the exercise of her functions and has powers to enforce the provisions of the DPA (including powers of investigation, entry and examination).

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**"

  Personal data relating 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**"

  Of, or in relation to, information or data, and 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**"

  A person who, either alone or with others, controls the content and use of personal data.

- "**Data Processor**"

  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 Subject**"

  An individual who is the subject of personal data.

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

  There is no definition of "Pseudonymous Data", "Direct Personal Data" and "Indirect Personal Data" in Irish law. The EU Data Protection Regulation (the "**GDPR**") which will apply from 25 May 2018, broadens the scope of the definition of "personal data".

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, including where the data are indirectly obtained by the controller (i.e., from a third party).

  The information to be provided 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;

  (c) any other information that is required to render the processing fair, having regard to the specific circumstances in which data are to be processed, and 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; and

  (d) where data are indirectly obtained, the categories of data and the identity of the original controller.

- **Lawful basis for processing**

  (A) Non-sensitive personal data:

  The legitimate processing grounds for non-sensitive personal data include the following:

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

  (b) confirmation that 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 non-contractual legal obligation to which the data controller is subject;

  iv. to prevent injury or other damage to the health of the data subject or 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 or under an enactment;

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

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

  vi. for the purposes of the legitimate interests pursued by the data controller (or third party to whom the personal data are disclosed), provided there is no unwarranted prejudice to the data subject.

  (B) Sensitive personal data:

  The legitimate processing grounds for sensitive personal data are more narrowly drawn, but include explicit consent of the data subject, processing which is necessary for exercising or performing legal rights and obligations of the controller in connection with employment, protection of vital interests, the administration of justice and for performing functions conferred by enactment or which are Government functions.

- **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 those purposes.

- **Data minimisation**

  The volume of personal data collected should not be excessive and be limited to what is directly relevant and necessary to accomplish a specific purpose.

- **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 ceases and the personal information is no longer required, the personal data must be deleted or disposed of in a secure manner.

- *Other key principles – please specify*

  The following key principles are also relevant:

  - **Data security**

    See question 13.1.

  - **Data transfers**

    Personal data must not be transferred from Ireland to a jurisdiction that is outside the EEA unless the country ensures an adequate level of data protection and/or at least one of a number of conditions permitting such a transfer is satisfied. See question 8.1 for further information relating to the conditions of transfer.

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, free of charge, to be informed if a data controller holds personal data about them. This includes the right to be given a description of the personal data and to be told the purposes for which their personal data are being held. A request for this information must be made in writing by the data subject and the data controller must provide the information within 21 days pursuant to the DPA.

  Section 4 of the DPA provides that data subjects have the right to obtain a copy of the personal data which relates to them that is held either on a computer or in a structured manual filing system or that is intended to form part of such a system. The data controller is given 40 days to provide a copy of the personal data to which the data subject is entitled and may charge a fee not exceeding €6.35.

  There are, however, exceptions to the right of access and the DPA sets out specific circumstances when a data subject's right of access to their personal data held by a data controller 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; or

  (d) hinder the assessment or collection of any taxes or duties.

  Certain personal data are also exempt from disclosure in certain circumstances if the information is:

  (a) protected by legal privilege;

  (b) back-up data;

  (c) 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;

  (d) an opinion on the data subject, given in confidence (in practice, this exemption is rarely relied upon);

  (e) used to prevent, detect or investigate offences, or will be used in the apprehension or prosecution of offenders; or

  (f) an estimate of damages or compensation regarding a claim against the data controller where disclosure is likely to cause damage to the data controller.

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

  Exemptions also apply in respect of access to social work data, and 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 the data subject to whom it relates. Data controllers and data processors who are healthcare providers must consult with the individual doctor before they disclose health data.

- **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 are not obtained lawfully or where it is inaccurate. The data controller or processor must respond within a reasonable amount of time and no later than 40 days after receipt of the request. There is no express right, however, for a data subject to have their personal data deleted, provided it is processed fairly in accordance with the DPA.

- **Objection to processing**

  Under section 6A of the DPA, data subjects have the right to object to processing which is likely to cause unwarranted damage or distress. This right applies where processing of the relevant personal data is necessary for the purpose of a legitimate interest pursued by the data controller to whom the personal data is, or will be disclosed or processing 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, following a request in writing, to require the data controller to cease processing data for direct marketing purposes. In situations where it is only retained for that purpose, they have the right to have the data erased which must be actioned by the data controller within 40 days. Under Regulations 13 and 14 of the E-Privacy Regulations, data subjects have the right to have their "opt-out" preference, which constitutes an objection to direct marketing to them, recorded in the National Directory Database (the "**NDD**").

- **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'.

- *Other key rights – please specify*

  - **Automated decision making**

    Data subjects have the right to object to decisions that have a legal or (other significant) effect on them which is based solely on processing of data which is intended to evaluate certain aspects of a person by automated means.

  - **Right to be forgotten**

    As a result of the *Google Spain* case in 2014, data subjects may have a 'right to be forgotten' in certain circumstances. While the DPC is yet to issue guidance on this, individuals can request that their data be erased where there is a problem with the underlying legality of the processing or where they withdraw their consent. The GDPR imposes a duty on the data controller to erase the relevant data or be subject to substantial fines for failure to comply.

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.)

It is mandatory for certain types of data processors and controllers to register with the ODPC if they hold personal data in an automated form and have a legal presence in Ireland, or use equipment located here.

There are, however, exceptions to this rule. Where an exemption applies, either under Section 16(1)(a) or (b) of the DPA or under S.I. No. 657 of 2007 – Data Protection Act 1988 (Section 16(1)) Regulations 2007 ("**S.I. No. 657 of 2007**"), it is limited only to the extent to which personal data are processed within the scope of that exemption.

Under the DPA, 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 and is open to consultation by the public in general or by any person demonstrating a legitimate interest;

(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 of their activities.

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

In addition, the following data controllers and data processors are not required to register (subject to certain conditions and the below comments on prescribed entities) in accordance with section 3 of S.I. No. 657 of 2007:

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

(b) solicitors and barristers who process data for the purposes of providing legal professional services;

(c) candidates for political office and elected representatives who process data for electoral activities;

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

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

i. advertising or marketing the data controller's business, activity, goods or services;

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

iii. deciding whether to accept any person as a customer or supplier;

iv. 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;

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

vi. performing a contract with the data subject, where the personal data are not processed other than where it is necessary to carry out such processing for any of the purposes set out above;

(f) 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 Act 2014;

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

(h) data controllers or data processors to which a code of practice approved under the DPA applies; and

(i) a data processor who provides data on behalf of a data controller insofar as the processing of the data would if undertaken by the data controller, fall under any one or more of paragraphs (a) to (h).

Certain prescribed entities, however, are required to register even where they would otherwise fall within one of the above exemptions (see question 5.3 for further details). Such prescribed entities include banks and financial/credit institutions, insurance undertakings (not including brokers), businesses engaged wholly or mainly in direct marketing, providing credit references or debt collection, internet access providers, and entities processing genetic data. In addition, any data processor who processes personal data on behalf of a data controller which is required to register, must also register with the DPC.

The ODPC is obliged not to accept an application for registration from a data controller which keeps sensitive personal data unless it 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 the controller. Where the ODPC refuses an application for registration, the applicant must be notified in writing of the reasons for the refusal. An appeal against such a decision of the ODPC may be made to the Irish Circuit Court.

The GDPR will abolish the requirement to register with a national supervisory authority.

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 and are not transferable from one data controller to another.

The DPA also provides that, where a data controller intends to keep personal data for two or more related purposes, it is only required to make one application in respect of those purposes. If, on the other hand, it intends to keep personal data for two or more unrelated purposes, it will need to make a separate application for each.

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 controller established in Ireland which cannot avail of an exemption specified in at question 5.1 must register with the ODPC.

The following categories of data controller and data processor are required to register, even if they would otherwise fall under any of the categories listed as exempt from registration in question 5.1 above:

- banks and financial/credit institutions;
- insurance undertakings (not including brokers);

- persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts;
- internet access providers;
- electronic communications network or service providers;
- persons who process genetic data; and
- data processors who process personal data on behalf of data controllers who fall under one or more of the above categories.

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.)

A data controller must provide a general statement of the nature of its business or trade or profession and of any additional purposes for which it keeps 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, email, staff ID number, etc.) must also be 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.

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 either directly or indirectly) 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.

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

Details of a 'compliance person' who will supervise the application of the DPA within the organisation must be given by data controllers and data processors.

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

Under the DPA, the sanctions include:

(a) fines:
  i. maximum of €3,000 on summary conviction; and
  ii. maximum of €100,000 on indictment; and

(b) a court order for forfeit, destruction and/or erasure of material which appears to be connected with an offence.

See also question 7.4 in relation to sanctions under the E-Privacy Regulations.

Under the DPA and the E-Privacy Regulations, officers of corporate bodies may in certain circumstances be guilty of an offence.

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 6–25 Employees (inclusive)	€100	€90
Applicants with 0–5 Employees (inclusive)	€40	€35

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

Registration must be renewed annually. A letter is sent by the ODPC as a reminder approximately three weeks prior to the date of renewal. Amendments may be upon renewal, free of charge – however, there is a fee for amendments during the year-long period.

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

Prior approval is 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 in relation to the procedure for obtaining prior approval.

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 ("**DPO**") is optional. When registering with the ODPC, however, both data controllers and processors must give details of a 'compliance person' within their organisation who will act as a contact point for the ODPC and supervise the application of the DPA within the organisation in relation to personal data.

Under the GDPR, any organisations whose core activities consist of regular and systematic monitoring of individuals on a large scale, or involve processing large amounts of sensitive personal data, will be required to appoint a DPO.

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

As there is no legal requirement to appoint a DPO, 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 DPO include:

(a) ensuring appropriate data protection expertise exists within an organisation and monitoring compliance with the DPA;

(b) improving data protection awareness, understanding the risks, rules, safeguards and rights in relation to processing personal data within the organisation;

(c) consistent and centralised handling of data subject access requests, audits and data breaches, with one contact point for all data protection-related issues;

(d) developing customer relationships and a reputation generally;

(e) building a relationship with the ODPC; and

(f) assisting with handling emergencies, such as audits or data breaches.

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

No specific qualifications are currently mandated by Irish law.

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 the DPO to ensure that the organisation complies with the DPA and to be the contact point for all such matters. The DPO provides support, assistance, advice and training to the employees of the organisation on data protection matters and inputs into the risk management processes of the organisation.

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

As there is no current legal requirement for an organisation to have a DPO, there is no notification obligation.

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.)

The rules governing marketing by post are mainly contained in the DPA. Marketing communications may be sent by post to either an individual or non-natural person (i.e. body corporate) customers or non-customers, unless they previously opt-out in writing. Marketing targets must always be given an option to opt-out, both at the time of data collection and on each occasion that marketing collateral is issued.

The E-Privacy Regulations set out the rules in relation to electronic communications.

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, for direct marketing purposes, 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. a body corporate) is allowed as long as they have not recorded their objection in the NDD (under "objection to marketing" under question 4.1 above), or they have not opted out of receipt of marketing.

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 NDD, or has opted out of receipt of direct marketing.

A 'soft opt-in' applies where an entity is marketing its own same or similar products or services to an existing customer, subject to certain conditions.

Direct marketing communications must include the name, address and telephone number of the marketer and the recipient must be given the right to opt-out of any subsequent marketing communication by a cost-free and easy method.

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

Yes. The DPC has pursued numerous prosecutions arising from breach of the E-Privacy Regulations.

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

The NDD contains details of subscribers who have expressed a preference not to receive marketing calls to landlines, or alternatively have positively indicated consent to receipt of marketing to mobile phones. Companies engaged in direct marketing calls by telephone should therefore consult the NDD, unless they have separate current marketing consents from the relevant data subjects.

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

The maximum penalties for sending marketing communications in breach of applicable restrictions are as follows:

- for communication by post:
  - a fine of €3,000 on summary conviction;
  - or €100,000 on indictment; or
- for electronic communications:
  - on summary conviction, a fine of €5,000; or
  - on indictment, a fine of €250,000 where the offender is a body corporate or in the case of a natural person, a fine of €50,000; and
  - a court order for the destruction or forfeiture of any data connected with the breach.

Under the E-Privacy Regulations, each breaching communication constitutes a separate offence.

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)?

Under the E-Privacy Regulations, consent is required for cookies which are not strictly necessary for a transaction that the data subject has explicitly requested. The user must be given clear information in relation to what the user is being asked to consent to in terms of cookie usage, and the means of consenting should be as user-friendly as possible. No particular form of, or means of obtaining consent is mandated and whether consent may be implied or express may depend on the circumstances.

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)?

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. See question 7.5.

7.7 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, but has not yet taken any public enforcement actions. In 2012, the ODPC wrote to 80 website operators seeking information on their consent procedures. Subsequently, in 2013, the ODPC liaised with the 80 websites to ensure compliance with the E-Privacy Regulations. The ODPC has also published guidance to assist companies and organisations which use cookies in order to achieve at least a minimum standard of compliance.

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

The maximum penalty for breaches of applicable cookie restrictions is a fine of €5,000 per offence 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 transfer of personal data to countries within the EEA.

Personal data, however, 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.

Even where one of the above elements exists, the DPC retains the power to prohibit the transfer of personal data abroad to any country (whether inside or outside the EEA) and may issue a prohibition notice which prevents transfer of data until certain steps have been taken.

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 mechanisms typically relied on by companies to transfer personal data abroad are:

(a) use of 'model clauses' between the data controller and the person/organisation to whom it intends to transfer the information to abroad. These are contractual clauses approved by the EU Commission which assure an adequate level of protection for the personal data. They do not require the approval of the ODPC. The ODPC can, however, approve transfers based on contractual clauses which do not directly conform to the model clauses (although this is rare);

(b) transfer to a country that is on the EU Commission 'adequate standard of protection' list (i.e., in respect of which there is a 'Community Finding'). See also question 16.2 in relation to recent developments concerning the EU-US Privacy Shield; or

(c) use of binding corporate rules ("**BCR**"), which enable personal data to be transferred to other companies within a group, as long as certain legally enforceable rules to protect personal data exist within the group. The BCRs are submitted to the ODPC or another data protection authority in another EEA jurisdiction for approval.

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.

If data are transferred abroad under contracts that vary from the 'model clauses', the transfer must be notified to and approved by the ODPC. There is no requirement to deposit the contracts with the ODPC once the process is complete. The ODPC will only consider authorising contracts that are general in nature, e.g. '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 or another data protection authority must also approve BCR mechanisms used to transfer data abroad where the transfers are within a corporate group. This requires engagement with the ODPC or another EEA data protection authority by the company involved. Use of BCRs has not, to date, been significant, given that the ODPC must review the BCRs in advance and it is considered to be a lengthy process. The 2015 Annual Report of the DPC indicates that in 2015, the ODPC was acting as the lead reviewer in four BCR applications and assisted the Belgian data protection authority with its assessment of a BCR application which has since been approved. The 2016 Annual Report has not been published at the time of writing.

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.)

The Whistle-Blowers Act covers both the public and private sectors and has been recognised as the highest level of protection available to whistle-blowers across the EU. Employers must now ensure that existing internal whistle-blower policies, and more generally, how they address such matters, are aligned with the requirements of the Whistle-Blowers Act. In accordance with international best practice, the safeguards in the Act are extended to a wide range of 'workers' and the concept of 'worker' is broadly defined to include employees (public and private sector), contractors, trainees, agency staff, former employees, jobseekers, and even certain individuals on work experience.

The Act provides an exhaustive list of 'relevant wrongdoings' (i.e., the scope of issues that may be reported) as follows:

(a) that an offence has been, is being or is likely to be committed;

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation, other than one arising under the worker's contract of employment or other contract whereby the worker undertakes to do or perform personally any work or services;

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur;

(d) that the health or safety of any individual has been, is being or is likely to be endangered;

(e) that the environment has been, is being or is likely to be damaged;

(f) that an unlawful or otherwise improper use of funds or resources of a public body, or of other public money, has occurred, is occurring or is likely to occur;

(g) that an act or omission by or on behalf of a public body is oppressive, discriminatory or grossly negligent or constitutes gross mismanagement; or

(h) that information tending to show any matter falling within any of the preceding paragraphs has been, is being or is likely to be concealed or destroyed.

There are no geographical boundaries for the commission of a wrongdoing. If an offence is committed abroad, but would not be regarded in that country as an offence, it will nonetheless qualify as a protected disclosure if it would be regarded as an offence under Irish law (and *vice versa*).

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?

The Whistle-Blowers Act imposes an obligation on the part of the recipient of a protected disclosure (and any person to whom a protected disclosure is referred in the course of the recipient's duties) not to disclose any information that may identify the person who made the protected disclosure, unless:

(a) the recipient can show that he/she took all reasonable steps to avoid disclosing any such information;

(b) the recipient reasonably believes that the person making the disclosure does not object to the disclosure of any such information;

(c) the recipient reasonably believes that disclosing such information is necessary for the effective investigation of the relevant wrongdoing; the prevention of serious risk to the security of the State, public health, public safety or the environment; or the prevention of crime or prosecution of a criminal offence; or

(d) the disclosure is otherwise necessary in the public interest or is required by law.

The Whistle-Blowers Act provides for a tiered disclosure regime with a number of avenues available to workers. The Whistle-Blowers Act encourages the vast majority of disclosures to be made to the employer in the first instance. However, other options are available where this is inappropriate or impossible.

Tier 1:

(a) *Internal disclosure to an employer or other responsible person*

A worker may make a protected disclosure to his employer where he/she reasonably believes that the information shows or tends to show relevant wrongdoing or, if the worker reasonably believes that the wrongdoing relates to the conduct of some person other than his/her employer (or to something for which some other person has legal responsibility), then the disclosure can be made to that person.

(b) *Disclosure to a Minister*

A worker employed in a public body may make a protected disclosure to a Minister of the Government on whom any function relating to that public body is conferred or disposed by or under any enactment. Public bodies are very broadly defined to include institutions of higher education and any entity on which any functions are conferred by or under any enactment (other than the Companies Act 2014).

(c) *Disclosure to a Legal Advisor*

A disclosure made in the course of obtaining legal advice (including advice relating to the operation of the Whistle-Blowers Act) from a barrister, solicitor, trade union or an official of an excepted body is protected. If this disclosure, however, is covered by legal professional privilege, a subsequent disclosure by the relevant adviser is not protected.

Tier 2:

The Minister for Public Expenditure and Reform may prescribe a list of 'prescribed persons' (e.g. a regulatory body) whose roles and responsibilities are defined by law and are, in the Minister's opinion, appropriate to receive and investigate matters arising from disclosures relating to any of the wrongdoings in relation to which a disclosure may be made.

The Whistle-Blowers Act contains a list of 72 prescribed persons, which largely consists of the heads of statutory bodies.

Where a worker chooses to disclose in this manner, in addition to having a reasonable belief that the disclosure tends to show one or more relevant wrongdoings, he must also have a reasonable belief that:

(a) the relevant wrongdoing falls within the description of matters as appears appropriate by reason of the nature of the responsibilities or functions of the relevant prescribed person; and

(b) the information disclosed, and any allegations contained in it, are true.

Tier 3:

There is also provision for disclosure in other circumstances (i.e., disclosure potentially into the public domain) where the standard for reporting is significantly higher. For this type of disclosure to be protected:

(a) the worker must reasonably believe that the information disclosed is substantially true;

(b) the disclosure cannot be made for personal gain (which does not include any reward payable under or by virtue of any enactment); and

(c) the making of the disclosure must be reasonable 'in all the circumstances'.

In addition, one or more of the following conditions must be met:

(a) at the time of making the disclosure the worker reasonably believes that he will be subject to penalisation by his employer if the disclosure is made to the employer;

(b) in a case where there is no prescribed person in relation to the relevant wrongdoing, the worker reasonably believes that evidence will be destroyed/concealed if a disclosure is made to the employer;

(c) the worker has previously made a Tier 1 disclosure of substantially the same nature, and no action was taken; and/or

(d) the relevant wrongdoing is of an exceptionally serious nature.

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.

No, corporate whistle-blower hotlines do not require separate registration/notification or prior approval from the ODPC.

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

There is no specific statutory requirement to have a separate privacy notice for whistle-blower hotlines, but in accordance with the data protection principles, the best practice is to put a privacy notice in place.

9.5 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 whistle-blower hotlines 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 information obtained in the future (e.g. in order to provide evidence).

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 make a separate registration/notification or prior approval with the ODPC 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 principal of proportionality, whereby employers must only collect relevant, adequate and non-excessive personal data, having regard to their legitimate aims.

Any employee monitoring by employers must strike an appropriate balance between the legitimate aims of the employer and the privacy rights of the employees in question. For instance, the constant monitoring of employees by CCTV would be difficult to justify, unless there was a specific security need for it. Employers should be certain that they will be able to meet their obligations to provide data subjects on request with copies of their captured images.

Employees have a legitimate expectation of privacy in relation to certain communications made from the workplace and any monitoring should be clearly set out in an applicable policy.

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 the purposes for which the data are processed. Surveillance of electronic communications and otherwise is often 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 for a separate registration, notification or prior approval with or from 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 provider should be able to give assurances on:

(a) continued access to data by the data controller (back-up and recovery measures);

(b) prevention of unauthorised 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 service 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 under the contract should include:

(a) a requirement that 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 are processed outside the EEA (where these are used is important that the protections afforded by these mechanisms also extend to the sub-processors).

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. It is strongly recommended, however, that thorough due diligence be undertaken as data protections issues may arise in many projects.

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 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. The ODPC, however, has published a non-binding Code of Practice entitled "*Personal Data Security Breach Code of Practice*" (the "**Code**"), which contains data security breach guidelines that include provisions relating to reporting and provides that all instances in which personal data has been put at risk should be reported to the ODPC as soon as the data controller becomes aware of the breach. The Code does not apply to providers of publicly available electronic communication networks or services, which are subject to mandatory reporting requirements under the E-Privacy Regulations (see question 13.3).

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. This is not required where:

(a) the breach affects fewer than 100 data subjects;

(b) the full extent and consequences of the incident have been reported, without delay, directly to those affected; and

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

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 affected data subjects 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 data 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.

Pursuant to the E-Privacy Regulations, providers of publicly available electronic communications networks must notify any individuals that may be adversely affected by the breach unless it has demonstrated to the DPC's satisfaction that it had implemented appropriate technological protection measures to the relevant data, which render the data unintelligible to any person who is not authorised to access it.

The Code, which applies outside the electronic communications industry, provides that data controllers must give immediate consideration to notifying the affected data subjects, unless there is no risk to the personal data because of the level of protection (e.g., by way of encryption), as outlined in question 13.2 above. The expectation of the ODPC is that the Code would be followed and, accordingly, in many instances that notification to data subjects would take place in accordance with the Code. The notification should include information on the nature of the personal data breach and a contact point where more information may be obtained, and should also recommend measures to mitigate the possible adverse effects of the breach.

13.4 What are the maximum penalties for security breaches?

Breach of the security principle in the DPA is not an offence. However, if the DPC was to issue an enforcement notice, or information notice, in respect of a breach which was not observed, such non-compliance would constitute a breach.

See question 5.5 in respect of sanctions in the case of an offence. Security breaches may also give rise to breach of the duty of care owed to data subjects, and therefore could give rise to a damages claim.

14 Enforcement and Sanctions

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

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

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 in question 14.1 on a regular basis. The ODPC has conducted investigations on, obtained information from, and conducted audits and inspections of, many organisations. During the course of 2015, the ODPC carried out 51 audit and inspections on major holders of personal data in the public and private sectors (which is a significant increase on the number carried out in 2014). The DPC is reported to have completed approximately 48 audits in 2016 and engaged in approximately 1,170 consultations. The 2016 annual report of the DPC is yet to be published.

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?

Where personal 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 to the Hague Conventions, the request will be 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 personal data.

Criminal Justice (Mutual Assistance) Acts 2008 and 2015 (the "Criminal Justice Acts")

The Criminal Justice Acts relate to requests for mutual assistance between Ireland and other EU Member States for co-operation in the policing of telecommunications messages for the purposes of criminal investigations. Furthermore, the Minister for Justice can now request that tapping of communications be undertaken in an EU Member State for an Irish-based criminal investigation, and also outlines how requests from other EU countries to Ireland for such interceptions should be processed.

Prior to the Criminal Justice Acts, a foreign State was restricted in what communications they could intercept legally in an Irish context. This was due to the wording of the Postal and Telecommunications Services Act 1983, and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 (the "**Interception Acts**"), which provide only for the interception of communications in respect of offences under Irish law. As the interception of communications involves the processing of personal data, the DPA also applied to all such interceptions. Exemptions under the DPA set out in section 8(b), where compliance with the DPA would prejudice the investigation, and section 8(e), where the processing is required by law or pursuant to a court order, were interpreted by the ODPC to apply only to Irish law, Irish ministerial orders and orders by the Irish courts. The mutual assistance regime established by the Criminal Justice Act now allows Ireland to share intercepted information with other EU Member States with the authorisation of the Minister for Justice and Equality, thereby satisfying the exemption criteria of the DPA.

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

The ODPC has not, as yet, issued official guidance in relation to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies. However, the Minister of State with special responsibility for data protection has previously expressed the view that the Irish Government has 'serious concerns' about the implications for Ireland and the EU arising from the US court decision in the *Microsoft* case. The Minister of State suggested that compliance with the warrant may result in Microsoft and any other US companies with operations in the EU which are served with such warrants in the future, being in breach of the DPA and the EU Data Protection Directive, stating that "*this would create significant legal uncertainty for Irish and EU consumers and companies regarding the protection of their data which, in this digital age, is everyone's most valuable asset*". The Irish Government has instead advocated the use of the existing mutual legal assistance treaty, which provides for assistance in legal cases or law enforcement investigations.

16 Trends and Developments

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

There has been a continued increase in data security breach notifications in the last 12 months, a large percentage of which were from the banking and financial services sector, and with the majority of these continuing to arise as a result of human error.

In all, there were 2,376 data security breach notifications submitted to the DPC in 2015 which was an increase of 112 from previous year. Data breach notifications will be mandatory under the GDPR, so it is likely that these notification numbers will change significantly.

This is consistent with a general increase in scrutiny on security of information generally, and cyber security in particular, as demonstrated by the publication in September 2016 by the Central Bank of Ireland of new guidance on information technology and cybersecurity, with the Central Bank indicating that it intends to strengthen further its supervisory capabilities of IT and cybersecurity in order to reduce cyber-attacks which are becoming increasingly more sophisticated and difficult to detect in the financial sector.

In that vein, the ODPC has also established a Special Investigations Unit (the "**SIU**") to carry out targeted and proactive investigations on its own initiative. The ODPC has to date targeted activities of private investigators, tracing agents and the sectors that use them and successfully prosecuted several investigators for privacy violations. It also provided assistance to the Office of the Information Commissioner in the UK in connection with similar investigations. The ODPC has notified relevant businesses of its investigations and continues working closely with the Private Security Authority (the regulatory body for the licensing of private investigators) to ensure the licensing standards take full account of the DPA.

The Irish Supreme Court, in its first ever data protection ruling handed down a decision in *Novak v Data Protection Commissioner*, deciding that the question "*is ultimately a matter of European law*" and referring the question to the Court of Justice of the European Union (the "**CJEU**") as to whether an exam script is capable of constituting personal data.

The DPC was successful in the High Court decision of *Martin v Data Protection Commissioner* whereby the powers and obligations of the DPC when investigating a complaint were clarified. The case centred on a complaint regarding an alleged verbal disclosure by a director of a credit union of details of the complainant's outstanding loans which the complainant asserted was in breach of his data protection rights, and concerned a request for an oral hearing before the DPC. The High Court found in favour of the DPC, ruling that there was no provision in the DPA entitling a data subject to an oral hearing before the DPC even where there is a conflict of evidence in a case. The Court held that in the absence of an express power, the Court should be slow to find that the DPC had an inherent power to hold such an oral hearing, as such power is a significant one and "*could not be said to be incidental to the powers of investigation conferred on the respondent and her staff*" by the DPA.

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

The hottest topic in Irish data protection law at present is GDPR, which was adopted on 24 May 2016 and will apply from 25 May 2018. It will replace the EU Data Protection Directive on which the DPA is based and bring a greater focus on accountability and transparency in processing and will introduce significant penalties for non-compliance. It will also introduce a 'one-stop shop' mechanism for multinational operations in Europe which will result in the functions of the ODPC evolving and being expanded. The DPC's 2015 annual report notes the significant progress in building the capacity and expertise of the ODPC through widespread recruitment, including specialist legal, technical, investigatory and communications experts, which reflects the increases in funding over the last few years, a trend which is expected to continue.

International data transfers continue to be an important focus for the ODPC.

The DPC commenced proceedings in the Irish High Court on 31 May 2016 seeking a reference to the CJEU in relation to the model clauses mechanism under which, at present, personal data may be transferred to countries outside of the EEA. The DPC is seeking a declaration as to the validity of the model clauses and is querying whether the model clauses effectively protect privacy rights of EU citizens, indicating the ODPC's view that the same shortfall noted by the CJEU in relation to the Safe Harbour may equally apply to the model clauses. The hearing before the High Court commenced on 7 February 2017.

The EU-US Privacy Shield, which was the solution to transatlantic data transfers following invalidation of the Safe Harbour programme by the CJEU in the 2015 Schrems decision, and which introduced a new framework for stronger obligations on US companies to protect personal data of European citizens, is also under scrutiny. Digital Rights Ireland, which is an Irish privacy advocacy group, has challenged the validity of the Privacy Shield before the European General Court, the lower of the CJEU. It could take a year or more for the European General Court to issue its ruling. Taking into account the number of changes and safeguards that have been introduced by GDPR, the EU-US Privacy Shield may in any event require adjustment.

Access requests also remain a hot topic. Enforced access requests are illegal as a matter of Irish law (i.e. requests made at the instance of an employer or potential employer to a data controller who holds data of the employee or potential employee (see question 1.2)). The ODPC is determined to clamp down on such requests and prosecute organisations who are engaged in such unlawful activities and has written letters to 40 organisations to determine their compliance with the rules.

Anne Marie Bohan
Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland

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

Anne-Marie Bohan is a partner in both the Innovation, Technology and FinTech Group and the Asset Management and Investment Funds Group at Matheson. Anne-Marie has extensive experience in outsourcing and managed service contracts, including transitional services contracts arising from business transfers, technology contracts and data protection, with specific focus on the requirements of financial institutions and service providers in these areas. Anne-Marie has advised on a significant number of complex multi-jurisdictional fund administration outsourcings and off-shorings, as well as domestic and cross-border fund mergers and consolidations. Anne-Marie's practice and cybersecurity issues, including data subject access requests and security breach incidents.

Anne-Marie has lectured on IT, data protection and financial services at the Law Society of Ireland, the National University of Maynooth, and more broadly. She is the author of the Ireland chapter in *Outsourcing Contracts – A Practical Guide* (A. Lewis, Fourth Edn. 2012) and is co-author of the Irish chapter in several data protection and Fintech related guides. Anne-Marie has recently been awarded the International Law Office (ILO) Client Choice Award 2017 (Ireland) for her work in IT and Internet Law.

Andreas Carney
Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland

Tel: +353 1 232 2837
Email: andreas.carney@matheson.com
URL: www.matheson.com

Andreas Carney is a partner in the Innovation and Technology Group and a member of the Data Protection and Privacy Group at Matheson. His core practice areas comprise outsourcing and other material service arrangements, data protection and IT. He works closely with clients from a diverse spread of industry sectors.

Andreas has advised extensively on IT infrastructure projects, including software and systems development, systems implementation and integration, systems support and maintenance, hardware supply, cloud services and co-location and other data centre arrangements. He also works regularly with clients in respect of their IT products and services, including social media, e-commerce and online consumer matters.

His data protection work is wide-ranging and includes strategic compliance advice, outsourced data processing arrangements, assisting clients in achieving privacy by design in new products and services, handling cross-border data flows, managing data security breaches, dealing with data subject access requests and representing clients on regulatory issues arising with the Irish Data Protection Commissioner.

Andreas is a committee member of the Ireland Group of the Society for Computers and Law.

Matheson

Matheson's primary focus is on serving the Irish legal needs of internationally focused companies and financial institutions doing business in and from Ireland. Our clients include over half of the Fortune 100 companies. We also advise seven 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 80 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 Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com