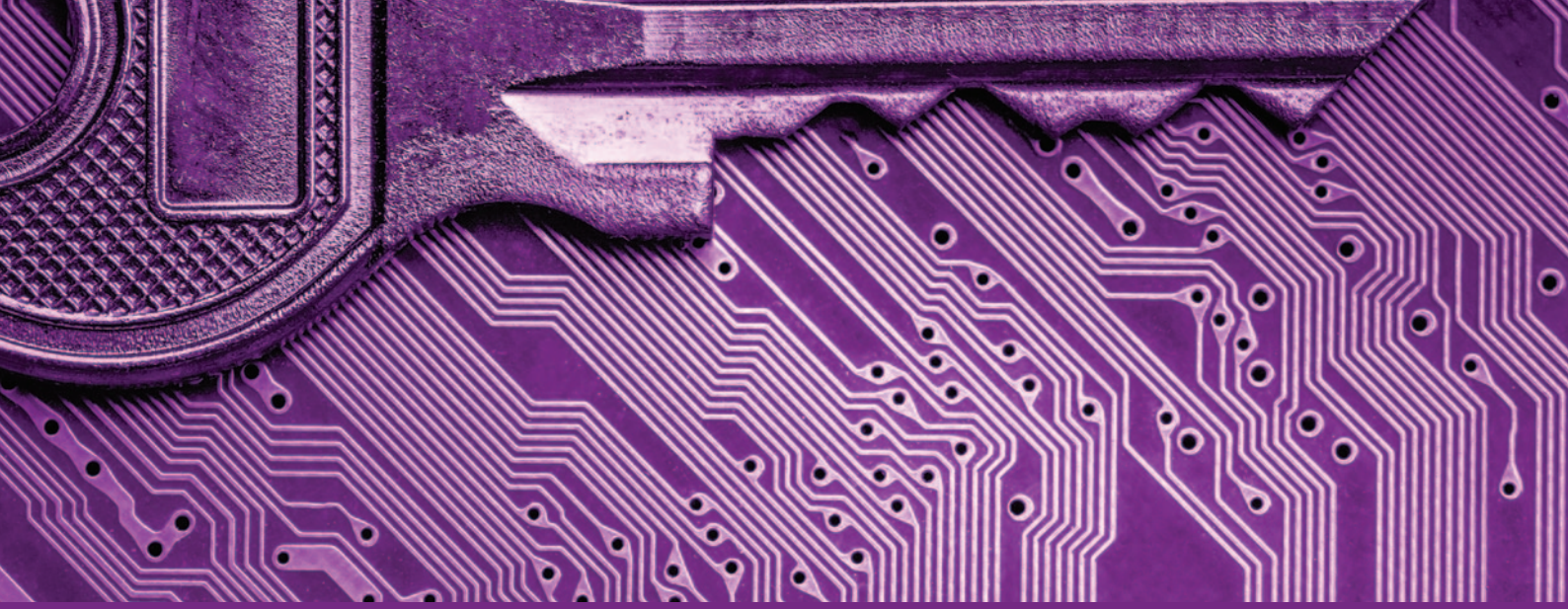

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
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
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

Ireland

Anne-Marie Bohan

Chris Bollard

Matheson

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in Ireland has been Regulation (EU) 2016/679 (the "**GDPR**"), as supplemented by the Data Protection Acts 1988 to 2018 (collectively the "**DPA**").

The GDPR repealed Directive 95/46/EC and has led to increased (although not complete) harmonisation of data protection law across EU Member States. Irish law-specific nuances, as permitted or required under the GDPR, are set out in the DPA, which also implements Directive (EU) 2016/680 (the Law Enforcement Directive).

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.
- The 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.

Data protection in the electronics communications sector is also subject to S.I. No. 336/2011 the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the "**2011 E-Privacy Regulations**"). The 2011 E-Privacy Regulations implement the provisions of three Directives, namely Directive 2002/58/EC, Directive 2006/24/EC, and Directive 2009/136/EC. The 2011 E-Privacy Regulations apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in Ireland and, where relevant, in the EU. The 2011 E-Privacy Regulations also contain provisions relating to electronic marketing, which apply generally to all organisations engaging in such activities.

The European Commission has issued a proposal for a Regulation on Privacy and Electronic Communications to replace the existing legislative framework, which would have direct effect on EU Member States (the "**Draft E-Privacy Regulation**"). However, this remains in draft form as at the date of this guide.

The DPA applies in relation to (i) the processing of personal data for the purposes of safeguarding the security of, or the defence or international relations of, the State, and (ii) the processing of personal data under the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 or the Vehicle Registration Data (Automated Searching and Exchange) Act 2018 (to the extent the Data Protection Act 1988 is applied in those Acts). The DPA also applies to complaints and investigations brought prior to the introduction of the GDPR.

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

The following sector-specific legislation impacts data protection:

- S.I. No. 188/2019 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019.
- S.I. No. 314/2018 – Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018.
- 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.

1.4 What authority(ies) are responsible for data protection?

The Data Protection Commission ("**DPC**") is the data protection supervisory authority responsible for ensuring that individuals' data protection rights are protected and that the GDPR is enforced. The DPC is independent in the exercise of its functions and has powers to enforce the provisions of the GDPR and DPA – see section 16.

2 Definitions

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

- "**Personal Data**"

  Any information relating to an identified or identifiable natural

person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- "**Processing**"

  Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- "**Controller**"

  The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- "**Processor**"

  A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- "**Data Subject**"

  An identified or identifiable natural person who is the subject of relevant personal data.

- "**Sensitive Personal Data**"

  The term "Sensitive Personal Data" is replaced under the GDPR with the term "Special Categories of Personal Data", being personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or sex life and sexual orientation.

- "**Data Breach**"

  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

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

The following terms are set out in the GDPR:

- "**Genetic data**" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- "**Biometric data**" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- "**Data concerning health**" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

There is no definition of "Pseudonymous Data", "Direct Personal Data" or "Indirect Personal Data" under Irish law. However, the term "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in Ireland (or any EU Member State), and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any EU Member State, but is subject to the laws of an EU Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses located outside the EU if they (either as controller or processor) process the personal data of EU residents in the context of: (i) offering of goods or services (whether or not in return for payment) to such EU residents; or (ii) monitoring of the behaviour of such EU residents (to the extent that such behaviour takes place in the EU).

The European Data Protection Board (the "**EDPB**") recently published Guidelines on the territorial scope of the GDPR (Guidelines 3/2018) which indicate that "establishment" extends to any real and effective activity (even a minimal one) exercised through stable arrangements (which, in some circumstances, could extend to the presence of a single employee or agent, if that employee or agent acts with a sufficient degree of stability).

4 Key Principles

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

- **Transparency**

  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

  The information must be provided at the time of collection of the personal data or, if the personal data is collected from a source other than the data subject, within a reasonable period after obtaining the personal data (and at the latest within one month).

- **Lawful basis for processing**

  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

The lawful bases for processing special categories of personal data are more narrowly drawn and such processing is only permitted under certain conditions, including the explicit consent of the data subject, where the processing is necessary in the context of employment law or for the protection of vital interests, and where the processing is necessary to assess the working capacity of an employee.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as described above.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**

  See 'Data minimisation' above.

- **Accuracy**

  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Other key principles – please specify

- **Data security**

  See response to question 15.1.

- **Accountability**

  The controller is responsible for, and must be able to demonstrate on request, compliance with the data protection principles set out above. This requires controllers and processors to have robust and documented processes and procedures to ensure ongoing good governance and record-keeping.

5 Individual Rights

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

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to make a complaint to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated decision-making that has a significant effect on the data subject. The information must be provided by the controller to the data subject free of charge and within one month of receipt of the request (except in limited circumstances).

  Additionally, the data subject may request a copy or a summary of the personal data being processed.

  There are exceptions to data subject rights, including the right of access, which are set out in the DPA. The restrictions on data subjects' access rights include where information is subject to legal privilege, were the information comprises an opinion of a third party given in confidence, or where personal data is processed for the purpose of estimating the amount of the liability of the controller on foot of a claim. In addition, the right of access to personal data must not adversely affect the rights of third parties.

- **Right to rectification of errors**

  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**

  Data subjects have the right to have their personal data erased (also known as the 'right to be forgotten') where: (i) the personal data is no longer necessary for the original purpose for which it was collected (and no new lawful basis for such processing exists); (ii) if the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful basis for such processing exists; (iii) the data subject exercises his/her right to object to processing, and the controller has no overriding grounds for continuing the processing; (iv) the personal data has been unlawfully processed; (v) erasure is necessary for compliance with EU law or national data protection law to which the controller is subject; or (vi) if the data subject is a child, the personal data has been collected in relation to the offer of information society services.

- **Right to object to processing**

  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. Where this right is exercised, the controller must cease such processing unless it is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**

  Data subjects have the right to restriction of processing of personal data (meaning the personal data may only be held by the controller, and may only be used for limited purposes) where: (i) the accuracy of the data is contested by the data subject (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for its original purpose of processing, but the data is still required by the controller for the establishment, exercise or defence of legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**

  A data subject has a right to receive a copy of certain of his/her personal data in a commonly used machine-readable format, and to be able to transfer (or have transferred directly on his/her behalf) his/her personal data from one controller to another.

- **Right to withdraw consent**

  A data subject has the right to withdraw his/her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**

  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing.

- **Right to complain to the relevant data protection authority(ies)**

  Data subjects have the right to lodge complaints concerning the processing of their personal data with the DPC if the data subject lives in Ireland or the alleged infringement occurred in Ireland.

Other key rights – please specify

- **Right to basic information**

  See question 4.1 (Transparency).

- **Breach notifications**

  Data subjects have the right to be informed of personal data breaches which are likely to result in high risk to their rights and freedoms.

- **Restrictions on data subject rights**

  None of the data subject rights set out in the GDPR is an absolute right, and each is subject to restrictions in certain circumstances, as specified in the GDPR and the DPA.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no requirement for a business to register or notify the DPC in respect of its processing activities. The previous requirement to register with the DPC was removed after the GDPR came into effect.

Data protection officers are required to be notified to the DPC (see question 7 below).

Whilst there is not an obligation to notify the DPC, where a business has appointed a representative pursuant to Article 27 of the GDPR (i.e., where the business is not established in the EU but is caught by the GDPR by virtue of offering goods or services to EU data subjects or monitoring the behaviour of data subjects located in the EU), that representative must be designated in writing and its details must be easily accessible to the DPC in order to facilitate the establishment of contact for cooperation purposes.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable; please see question 6.1 above.

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

This is not applicable; please see question 6.1 above.

6.4 Who must register with/notify the data protection authority (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)?

This is not applicable; please see question 6.1 above.

6.5 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)?

This is not applicable; please see question 6.1 above.

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

This is not applicable; please see question 6.1 above.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable; please see question 6.1 above.

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

This is not applicable; please see question 6.1 above.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable; please see question 6.1 above.

6.10 Can the registration/notification be completed online?

This is not applicable; please see question 6.1 above.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable; please see question 6.1 above.

6.12 How long does a typical registration/notification process take?

This is not applicable; please see question 6.1 above.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is mandatory for public authorities and for organisations whose core activities consist of (i) data processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale, or (ii) processing on a large scale of special categories of personal data or criminal convictions.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR in respect of data protection officers apply as though the appointment were mandatory.

In general, Irish law does not prescribe for the appointment of a Data Protection Officer beyond the requirements of the GDPR.

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

Failure to appoint a Data Protection Officer where required (or a breach of other provisions of the GDPR relating to such appointment) may result in an administrative fine of up to €10 million or 2% of annual global turnover.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Yes, the Data Protection Officer is an independent advisory function and must be free from disciplinary measures or other employment consequences for performing his/her tasks. He/she must also be free from conflicts of interest, must not receive any instructions in carrying out the function and must have access to the highest level of management in the organisation.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, group companies may jointly appoint a Data Protection Officer, provided that the Data Protection Officer is easily accessible by each member of the group. The role may also be outsourced to a third party.

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

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. The DPC has published some guidance on appropriate qualifications for a Data Protection Officer on its website.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

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

Yes, the DPC must be notified and details of the DPO provided to it.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Although it is not strictly required to name the Data Protection Officer (on an individual basis) in a public-facing privacy notice, the contact details of the Data Protection Officer must be notified to the data subject at the point the personal data is collected (so as a matter of practice, most organisations include the contact details, although not necessarily the name, of the Data Protection Officer in the privacy notice).

As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the EDPB) recommended in its 2017 guidance on Data Protection Officers that both the DPC and employees within the organisation should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business), along with certain prescribed provisions set out in Article 28 of the GDPR.

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The agreement should set out the subject matter, the duration, the nature and purpose of the processing, the types of personal data and categories of data subjects and the obligations and rights of the controller.

The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes

confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in meeting its data security, breach notification and data protection impact assessment obligations; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The 2011 E-Privacy Regulations set out the rules in relation to electronic communications. The underlying principles of the GDPR must also be observed with regard to personal data processed for marketing purposes.

When using email or SMS to send messages to an individual for direct marketing purposes, the data subject's prior opt-in consent must be obtained. Consent should meet the standard set out in the GDPR. However, 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. In limited circumstances, it may also be possible to market to business email addresses, unless the recipient objects.

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

It is an offence under the 2011 E-Privacy Regulations to send communications without the requisite permissions.

The Draft E-Privacy Regulation will replace the 2011 E-Privacy Regulations once in force.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

As per question 9.1 above, when using automatic dialling machines or fax 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 National Directory Database ("**NDD**"), or they have not opted out of receipt of direct 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.

Where marketing materials are sent by post, data subjects have the right to object at any time to processing of personal data for direct marketing purposes. The right to object must be explicitly brought to the attention of the data subject and presented clearly and separately from any other information. Personal data must not be processed for marketing purposes where the data subject has objected to such processing.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The 2011 E-Privacy Regulations apply to the processing of personal data in connection with publicly available electronic communications services in public communications networks in Ireland and the European Community, so marketing sent from jurisdictions within the European Community are captured.

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

Yes, the DPC is, and traditionally has been, active in this area. By way of example, the DPC recently conducted an audit of a professional networking organisation in Ireland after becoming concerned with its use of non-member email addresses to engage in targeted advertising. The complaint was resolved amicably but demonstrates the DPC's proactive approach in this area. A number of other investigations made under the 2011 E-Privacy Regulations concluded with successful District Court prosecutions by the DPC (against five entities in respect of a total of 30 offences).

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Although it is not unlawful in itself to purchase marketing lists, organisations may only contact the individuals on such marketing lists where those individuals have specifically consented (at the time their contact details were collected) to receipt of marketing communications and to the sharing of their personal data for those purposes (subject to the 'soft opt-in' described under question 9.1 above). In practical terms, the circumstances in which an organisation will be entitled, under the GDPR and the 2011 E-Privacy Regulations, to make use of a marketing list purchased by it, will be limited.

In respect of telephone calls, the NDD (see question 9.2 above) 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 using bought-in lists to engage in direct marketing calls by telephone should therefore consult the NDD (and any internal lists of numbers which should not be contacted) in advance of the use of any purchased lists.

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

Under the 2011 E-Privacy Regulations, it is an offence to send electronic communications in breach of applicable restrictions. The penalties for such offences are:

- 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.

A court order for the destruction or forfeiture of any data connected with the breach may also be issued. Each breaching communication constitutes an independent offence under the 2011 E-Privacy Regulations.

There is some overlap between the 2011 E-Privacy Regulations and the GDPR. Where a breach of the GDPR occurs in relation to the sending of marketing communications (for example, where the appropriate level of consent has not been sought), the business may be subject to an administrative fine under the GDPR.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Under the 2011 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 he/she is being asked to consent to in terms of cookie usage, and the means of consenting should be as user-friendly as possible.

The Draft E-Privacy Regulation, when in force, will replace the 2011 E-Privacy Regulations.

The forthcoming decision of the Court of Justice of the European Union in the Planet49 case will provide further guidance on cookie transparency and consent.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Under the 2011 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 he/she is being asked to consent to in terms of cookie usage, and the means of consenting should be as user-friendly as possible. Consent is not required where cookies are strictly necessary to provide the service being sought (for example, in order to provide a functioning website).

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

The DPC has been active in this field, but has not yet taken any public enforcement actions. The DPC has also published guidance on its website to assist companies and organisations which use cookies.

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

The penalties for breaches of applicable cookie restrictions under the 2011 E-Privacy Regulations are as follows:

- 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.

A court order for the destruction or forfeiture of any data connected with the breach may also be issued.

As discussed above, there is some overlap between the 2011 E-Privacy Regulations and the GDPR. Where a breach of the GDPR occurs in relation to the placement of cookies (for example, where the appropriate level of consent has not been sought), the business may be subject to an administrative fine under the GDPR.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Personal data may not be transferred from Ireland outside the European Economic Area ("**EEA**") unless one of the following applies:

(a) the personal data is transferred to a jurisdiction in respect of which a finding of adequacy has been made by the European Commission (see also question 11.2 in relation to the EU-US Privacy Shield);

(b) the transfer is made on the basis of the European Commission's pre-approved standard contractual clauses between the controller and the person/organisation to whom it intends to transfer the information abroad, which ensure an appropriate level of protection for the personal data (which do not require the approval of the DPC);

(c) the transfer is made on the basis of intra-group binding corporate rules ("**BCRs**"), which have been approved by the DPC or another data protection supervisory authority in another EEA jurisdiction;

(d) the transfer is made on the basis of an approved code of conduct pursuant to Article 40 of the GDPR, together with binding and enforceable commitments of the organisation in the third country to apply the appropriate safeguards, including as regards data subject rights;

(e) the transfer is made on the basis of an approved certification mechanism pursuant to Article 42 of the GDPR, together with binding and enforceable commitments of the organisation in the third country to apply the appropriate safeguards, including as regards data subject rights;

(f) the transfer is made pursuant to a legally binding and enforceable instrument between public authorities or bodies; or

(g) one of the derogations specified in the GDPR applies to the relevant transfer (in limited circumstances).

Following the withdrawal of the United Kingdom from the European Union, the United Kingdom will become a 'third country' for the purposes of data protection law and, unless a finding of adequacy is made by the European Commission, one of the safeguarding mechanisms described above must be implemented in respect of transfers of personal data from the EEA to the United Kingdom.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

See question 11.1.

Transfers of personal data to the United States of America ("US") are permitted where the US entity receiving the personal data has signed up to the EU-US Privacy Shield framework, which was designed by the US Department of Commerce and the European Commission to provide businesses in the EU and the US with a mechanism to facilitate the transfer of personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Where transfers of personal data to other jurisdictions are made pursuant to standard contractual clauses approved by the European Commission, the DPC does not need to be notified of the transfer.

If personal data is transferred outside the EEA under contracts which vary the provisions of the standard contractual clauses, the transfer must be notified to and approved by the DPC. There is no requirement to deposit the contracts with the DPC once the process is complete. The DPC will only consider authorising contracts that are general in nature (e.g. standard contractual clauses that can be relied upon by a number of different controllers within a sector or category, rather than specific contracts). The length of time this process takes varies depending on the nature of the modifications to the standard contractual clauses.

The DPC or another data protection authority must approve BCRs which are intended to be used to transfer personal data outside the EEA within a corporate group. This requires engagement with the DPC or another EEA data protection authority by the organisation involved. Use of BCRs has not, traditionally, been significant, given that the DPC must review the BCRs in advance and it is considered to be a lengthy process. However, the Annual Report of the DPC covering the period 25 May 2018 to 31 December 2018 indicates that the DPC has continued to act or has commenced acting as lead reviewer on 11 BCR applications.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistleblowers Act covers both the public and private sectors and has been recognised as providing significant levels of protection to whistle-blowers across the EU. Employers must ensure that existing internal whistle-blower policies, and more generally, how they address such matters, are aligned with the requirements of the Whistleblowers 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, independent contractors, trainees, agency staff, and certain individuals on work experience.

The Whistleblowers 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.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The Whistleblowers Act imposes an obligation on the part of the recipient of a protected disclosure 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 Whistleblowers Act provides a number of avenues to workers for making a protected disclosure.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV does not require prior approval from the DPC. However, controllers or processors using CCTV must comply with their general obligations under the GDPR in the use of CCTV cameras and footage (including that such processing must have a lawful basis). Appropriate notification must be given to individuals who may be recorded via CCTV cameras (e.g. a visible sign or in an applicable policy).

The DPC, in its Annual Report covering the period from 25 May 2018 to 31 December 2018, indicated that its Special Investigations Unit has opened 31 own-volition inquiries under the DPA into the surveillance of citizens by the state sector for law enforcement purposes through the use of technologies including CCTV.

13.2 Are there limits on the purposes for which CCTV data may be used?

See question 13.1 above in relation to compliance with data protection obligations.

14 Employee Monitoring

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

There are no particular restrictions around the types of monitoring which may be used in respect of employees (e.g. monitoring of electronic communications or surveillance by CCTV). However, given that the act of monitoring involves the collection of personal data, the principles outlined in question 4.1 above must be adhered to (particularly the principles around transparency and proportionality).

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 example, consistent monitoring of employees by CCTV would be difficult to justify, except where there is a specific security need. 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.

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

Employees must be notified of the existence of monitoring and the purposes for which the data are processed (which is usually achieved through an appropriate privacy notice). While consent is not required, the employer must have a lawful basis for the monitoring, which must be proportionate. Covert monitoring is almost never justified, with the possible exception of criminal investigations.

14.3 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).

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, there is a general obligation under the GDPR to ensure the security of processing of personal data.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, organisations must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

Depending on the risk, such measures may include (as appropriate): (i) pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems and services; (iii) an ability to restore the availability and access to personal data in a timely manner following a technical or physical incident; and (iv) a process for regularly testing, assessing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 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) expect(s) voluntary breach reporting.

Yes, a controller must report a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the DPC, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification by the controller to the DPC must describe the nature of the personal data breach including the categories and number of data subjects concerned, communicate the name and contact details of the Data Protection Officer or relevant point of contact, describe the likely consequences of the breach and describe the measures proposed to be taken by the controller to address and/or mitigate the breach.

15.3 Is there a legal requirement to report data breaches to affected data subjects? 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) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate a breach to affected data subjects without undue delay, where the breach is likely to result in a high risk to the rights and freedoms of the data subjects.

The communication must describe in clear and plain language the nature of the personal data breach, include the name and contact details of the Data Protection Officer (or point of contact), describe the likely consequences of the breach, and describe any measures proposed to be taken by the controller to address and/or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts), or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €10 million or 2% of global annual turnover.

16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigation Powers	The DPC (and its authorised officers) has broad powers under the DPA to enter business premises, including the right to: (i) access, search and inspect any premises where processing of personal data takes place and the documents, records, statements or other information found there; (ii) require any employees to produce any documents, records, statements or other information relating to the processing of personal data (or direct the authorised officers to where they might be located); (iii) secure for later inspection any documents, records, equipment or place in which records may be held; (iv) inspect, take extracts, make copies or remove and retain such documents and records as considered necessary; and (v) require any person referred to in (iii) above to give the authorised officer any information relating to the processing of personal data that the officer may reasonably require for performing his/her functions. The DPC may also conduct investigations in the form of data protection audits, issue information and enforcement notices (and require the controller/processor to take certain steps specified in the enforcement notice), require the controller/processor to provide a report on any matter, and, where it considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, apply to the High Court for an order suspending, restricting or prohibiting processing.	Where a controller or processor (or any person) fails to comply with an information or enforcement notice, or obstructs or impedes, or refuses to comply with a request from, an authorised officer, it shall be guilty of an offence and liable: (a) on summary conviction, to a fine of up to €5,000 and/or imprisonment for up to 12 months; and (b) on indictment, to a fine of up to €250,000 and/or imprisonment for up to five years.
Corrective Powers	The data protection authority has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification, and to impose an administrative fine (as below).	Not applicable.
Authorisation and Advisory Powers	The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.	Not applicable.
Imposition of administrative fines for infringements of specified GDPR provisions	The GDPR provides for administrative fines which can be up to €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year.	Not applicable.
Non-compliance with a data protection authority	The GDPR provides for administrative fines which can be up to €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher.	See 'Investigation Powers' above in relation to certain offences.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR and the DPA entitle the DPC to impose a temporary or definitive limitation, including a ban on processing.

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

The DPC exercises all of the powers referred to in question 16.1 on a regular basis. The DPC has conducted investigations on, obtained information from, and conducted audits and inspections of, many organisations. The DPC carried out 20 audits and inspections on major holders of personal data in the public and private sectors between 1 January and 24 May 2018. It also indicated in its Annual Report, covering the period from 25 May 2018 to 31 December 2018, that its Special Investigations Unit has opened 31 own-volition inquiries under the DPA into the surveillance of citizens by the state sector for law enforcement purposes through the use of technologies including CCTV.

Since 25 May 2018, the DPC has opened 15 statutory enquiries in relation to multinational technology companies' compliance, and 35 in relation to Irish companies' compliance, with the GDPR.

In 2018, the DPC commenced a project to develop a new five-year regulatory strategy, which will include extensive external consultation during the course of 2019.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The DPC has the ability under the GDPR to enforce against businesses established in other jurisdictions where such businesses fall within the scope of the GDPR (i.e., where they are carrying out processing activities related to the offering of goods or services to, or monitoring the behaviour of, data subjects in the EU). The DPC is able to enforce its powers through the business's representative, which is required to be appointed pursuant to Article 27 of the GDPR.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically 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 them. 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.

17.2 What guidance has/have the data protection authority(ies) issued?

The DPC has not, as yet, issued official guidance in relation to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

18 Trends and Developments

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

There have been over 2,860 complaints submitted to the DPC since 25 May 2018 (of which the GDPR applies to approximately 2,000). Complaints in relation to data access requests account for the highest volume of complaints, making up 977 of the complaints filed. Additionally, cross-border issues, rights of erasure and deletion are emerging as a significant category of complaints.

The DPC has issued 18 formal decisions since 25 May 2018. Of these, 13 upheld the complaint and five rejected the complaint. A number of investigations made under the 2011 E-Privacy Regulations concluded with successful District Court prosecutions by the DPC against five entities in respect of a total of 30 offences.

The DPC is engaged in ongoing litigation with Facebook in the Supreme Court on the validity of standard contractual clauses.

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

Brexit is a key focus area at present. The DPC issued guidance in December 2018 clarifying that in the event of a 'hard' Brexit, where the United Kingdom leaves the EU without the Withdrawal Agreement being implemented, the United Kingdom will become, with immediate effect, a 'third country' for the purposes of the GDPR. Without a finding of adequacy by the European Commission (or similar arrangement to permit the lawful transfer of data to the United Kingdom without a finding of adequacy), organisations transferring personal data from the EEA to the United Kingdom will accordingly be required to put in place a safeguarding mechanism. See question 11.1. The DPC has commented that approximately 70% of small and medium-sized enterprises in Ireland have never traded outside the EU and are accordingly unfamiliar with the international transfer mechanism. The DPC has produced templates to assist such organisations in achieving compliance with the requirements by the date on which the United Kingdom leaves the EU, if required. If the Withdrawal Agreement does come into effect, the *status quo* will remain while negotiations take place.

Data breaches are another focus area. Between 25 May 2018 and 31 December 2018, the DPC received 3,687 data breach notifications and handled 48 data breach complaints, including a number of complaints against the Central Statistics Office in relation to the disclosure of P45 details.

The DPC has expressed interest in CCTV recording, dashcams and bodycams (having published recent guidance on these topics) as well as 'connected vehicles', and it is anticipated that the DPC will be actively looking at organisations operating in these spaces. It is also running consultations at present on children's rights and the DPC's regulatory strategy.

Overall, there is an enhanced awareness of data subject rights and a rise in the uptake and exercise of those rights.

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 has over 20 years' experience in technology-related legal matters, and is Head of Matheson's Technology and Innovation Group and a member of our Asset Management and Investment Funds Group. Anne-Marie brings together significant practical experience in advising on technology and privacy legal issues, with industry knowledge and an understanding of applicable regulatory rules and regulatory requirements. She advises on all aspects of technology and e-commerce law, as well as outsourcings and contracted services, with particular 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 highest-value and most complex outsourcing contracts for IT and telecommunications systems and services, including advising on a number of the most significant financial services outsourcings in Ireland.

Chris Bollard
Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland

Tel: +353 1 232 2273
Email: chris.bollard@matheson.com
URL: www.matheson.com

Chris Bollard is a partner in the Technology and Innovation team. Chris advises clients on a host of data protection, information technology, e-commerce and intellectual property issues.

Chris advises local and international companies on compliance with data protection laws, including GDPR compliance, data processing agreements, international data transfers, data protection impact assessments and data access requests. Chris has particular experience advising international, data-rich companies who are doing business in Ireland.

Chris is a frequent speaker on data protection matters. He lectures on the Law Society of Ireland's Certificate in Data Protection Law course, as well as the Diploma in Technology Law course.

Chris also advises on the protection and commercialisation of intellectual property, including software licences, software development agreements, intellectual property assignments and intellectual property transfers in the context of mergers and acquisitions.

On the e-commerce side, Chris is frequently called on to advise companies selling goods and services online. As well as the core of IT/DP and IP issues, Chris also advises on more niche regulatory matters such as gambling law, the law relating to promotions and advertising, e-signatures and the Commercial Agents Directive.

Matheson has the longest established technology law practice in Ireland, set up more than 20 years ago. Over that period, we have advised the tech sector and blue-chip technology companies in Ireland, including multi-nationals in relation to their technology-related work, consistently and with a specialised focus, and have been involved at the cutting edge of technology-related legal developments. The Technology and Innovation Group's expertise spans the full spectrum of technology infrastructure, products and services.

Our specialised team of technology-focused lawyers have a breadth and depth of transactional and advisory experience that is unrivalled. We act for some of the largest multinational ICT companies with operations in Ireland, as well as some of the main corporate and public sector users of information technology in the country, and have advised on many of the largest and most complex IT, computer and systems integration, outsourcing, cloud computing and managed services contracts in Ireland. We advise a large number of software, hardware, technology and internet multinational organisations, and are involved in both national and international technology legal work, as well as in some of the largest technology-based transactions and initiatives in Ireland.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- 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
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State 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 Investment Funds
- 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