International
Comparative
Legal Guides

Data Protection 2021

A practical cross-border insight into data protection law

Eighth Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Arthur Cox LLP
Chandler MHM Limited
CO:PLAY Advokatpartnerselskab
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
FABIAN PRIVACY LEGAL GmbH
Foucaud Tchekhoff Pochet et Associés (FTPA)
H & A Partners
in association with Anderson Mōri & Tomotsune
Hajji & Associés
Hammad and Al-Mehdar Law Firm
Homburger
Iriarte & Asociados
Khaitan & Co LLP
King & Wood Mallesons
Klochenko & Partners Attorneys at Law
Koushos Korfiotis Papacharalambous LLC
Law Firm Pirc Musar & Lemut Strle Ltd
Lee and Li, Attorneys At Law
Leśniewski Borkiewicz & Partners
LPS L@W
LYDIAN
McMillan LLP
MinterEllison
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
Nikolinakos & Partners Law Firm
OLIVARES
Pinheiro Neto Advogados
PLANIT // LEGAL
S. U. Khan Associates Corporate & Legal Consultants
SEOR Law Firm
White & Case LLP
Wikborg Rein Advokatfirma AS

ICLG.com

ISBN 978-1-83918-127-6
ISSN 2054-3786

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Data Protection 2021

Eighth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

ICLG.com

Ireland

Colin Rooney

Aoife Coll

Arthur Cox LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The primary data protection legislation in Ireland is Regulation (EU) 2016/679 (the "**GDPR**"), and the Data Protection Acts 1988 to 2018 (together the "**DPA**"). Irish law-specific requirements which are required or provided for under the GDPR, are set out in the Data Protection Act 2018. The Data Protection Act 2018 also implements Directive (EU) 2016/680, the Law Enforcement Directive.

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

Yes. The following legislation also impacts data protection in Ireland:

- The Freedom of Information Act 2014 provides a legal right for persons to access information held by a body to which FOI legislation applies.
- The Protected Disclosures Act 2014 (the "**Protected Disclosures Act**") provides employment protections and certain legal immunities to workplace whistle-blowers.
- The Criminal Justice (Mutual Assistance) Act 2008, Part 3 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 "**ePrivacy Regulations**"). The ePrivacy 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 ePrivacy Regulations also contain provisions relating to electronic marketing.

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

The following sector-specific legislation impacts data protection:

- S.I. No. 18/2021 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021.
- S.I. No. 534/2020 – Data Protection Act 2018 (section 60(6)) (Central Bank of Ireland) Regulations 2020.
- S.I. No. 730/2020 – Protection of Employees (Employers' Insolvency) Act 1984 (Transfer of Personal Data) Regulations 2020.
- S.I. No. 537/2019 – Data Protection Act 2018 (Section 60(6)) (Central Bank of Ireland) Regulations 2019.
- 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 of Ireland (the "**DPC**"). The DPC is responsible for enforcing the GDPR and the DPA.

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 living natural person who is the subject of relevant personal data.
- "**Sensitive Personal Data**"
  The term "Sensitive Personal Data" was 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")*
  "Pseudonymous Data", "Direct Personal Data" or "Indirect Personal Data" are not defined under Irish law. "Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a 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 organisations that are established in Ireland (or any EU Member State), that process personal data (regardless of whether the processing takes place in the EU). An organisation 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, must also comply with the GDPR. The GDPR applies to organisations located outside the EU if they (either as controller or processor) process the personal data of EU residents through:

(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).

4 Key Principles

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

- **Transparency**
  Transparency demands that data processing be undertaken in a transparent manner and data subjects are provided with certain information in relation to the processing of their personal data. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and precise language. Data subjects must be provided with this information 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 time period after obtaining the personal data (and at the latest within one month).
- **Lawful basis for processing**
  Processing of personal data must be grounded on one or more lawful bases under Article 6 GDPR. The following lawful bases are the most relevant for organisations:
  (i) prior, freely given, specific, informed and unambiguous consent of the data subject. It must be as easy to withdraw consent as it was to give consent;
  (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 to perform the relevant processing); or
  (iv) legitimate interests (i.e. the processing is necessary for the purposes of legitimate interests of the controller or a third party except where those interests are overridden by the interests, fundamental rights or freedoms of the data subjects).
- **Purpose limitation**
  Purpose limitation is the principle that personal data is processed only for the particular purpose(s) for which it was collected (and for closely related purposes)). Personal data 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 before such processing is undertaken; and
  (ii) be able to rely on a lawful basis.
- **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.
- **Proportionality**
  See "Data Minimisation" above.
- **Retention**
  Personal data is not to be kept in an identifiable form for any longer than the purposes for which it was collected (subject to certain limited exceptions).
- *Other key principles – please specify*
  - **Accountability**
    The principle of accountability requires that controllers are able to demonstrate compliance with each of their obligations under the GDPR.
  - **Integrity and confidentiality**
    This principle requires that technical and organisational security measures be put in place to ensure personal data is protected from various forms of data breaches.

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 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 to the data subject free of charge and within one month of receipt of the request (except in certain limited circumstances wherein the deadline may be extended by a further two months).

The data subject may also request a copy or a summary of the personal data being processed. The DPA contain exceptions to data subject rights, including the right of access. The restrictions on the right of access include where the personal data is legally privileged. Under Article 15(4) GDPR the right of access to personal data must not adversely affect the rights and freedoms of others.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data is erased or rectified.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to have their personal data 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 to processing of their personal data where the lawful basis for that processing is public interest or legitimate interest. Where a data subject relies on this right, the controller must cease processing unless it can 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 (i.e. the personal data may only be used for limited purposes by the controller) where:
  (i) the accuracy of the data is contested by the data subject (for as long as it takes to verify that accuracy);
  (ii) the processing is unlawful and the data subject requests restriction (where the data subject opposes 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**
  In certain circumstances, a data subject has a right to receive a copy of certain of his/her personal data in a structured, commonly used and 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 to processing at any time. Data subjects must be informed of the right to withdraw consent before consent is provided and it must be as easy for a data subject to withdraw consent as it was for the data subject to give it. The lawfulness of processing based on consent before its withdrawal is not affected by its withdrawal.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing at any time. This includes profiling to the extent it relates to such direct marketing.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to complain to the relevant data protection authority(ies). In Ireland the data protection authority is the DPC.
- *Other key rights – please specify*
  - **Right to basic information**
    See question 4.1 (Transparency).
  - **Restrictions on data subject rights**
    None of the data subject rights set out in the GDPR is an absolute right. Each is subject to restrictions in certain circumstances, as specified in the GDPR and/or 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 on a business to register with or to notify the DPC of its data processing activities.

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)?

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)?

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)?

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)?

Not applicable. Please see question 6.1 above.

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

Not applicable. Please see question 6.1 above.

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

Not applicable. Please see question 6.1 above.

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

Not applicable. Please see question 6.1 above.

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

Not applicable. Please see question 6.1 above.

6.10 Can the registration/notification be completed online?

Not applicable. Please see question 6.1 above.

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

Not applicable. Please see question 6.1 above.

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

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.

It is mandatory to appoint a Data Protection Officer ("**DPO**") for public authorities and for organisations whose core activities consist of: (i) data processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (ii) data processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

There is no requirement under Irish law to appoint a DPO outside of the requirements set out in the GDPR.

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

An administrative fine of up to €10 million or 2% of worldwide annual 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 DPO cannot be dismissed or penalised for performance of his/her tasks as the DPO is an independent advisory function.

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

Yes. A group of undertakings may appoint a single DPO. The DPO must be easily accessible from each undertaking.

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

The DPO should have an expert knowledge of data protection law and practices and the ability to carry out his/her required tasks. An organisation is required to support the DPO by providing resources necessary for the DPO to carry out his/her tasks. The DPC has published guidance on its website on the role of DPOs including the relevant skills and expertise a DPO should have.

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

A DPO should be involved in all issues relating to the processing of personal data. The GDPR outlines the minimum tasks that a DPO should have:

(i) informing and advising a controller, processor and their employees who process personal data, of their obligations under the GDPR;

(ii) monitoring compliance with the GDPR, national data protection legislation and internal policies regarding the processing of personal data, including awareness-raising and training of staff;

(iii) advising on data protection impact assessments; and
(iv) cooperating with the DPC and acting as a contact point for the DPC.

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

Yes. The DPO must be registered with the DPC.

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

No. Contact details must be provided but it is not necessary to name the DPO.

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. A controller and processor are required to enter into a written agreement. This agreement must contain certain specific provisions that are set out in Article 28 GDPR as well as information in relation to the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and the categories of data subjects.

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.)?

It is necessary to enter a binding written agreement. This should set out the subject-matter, duration, nature and purpose of the processing. The agreement should also cover the type of personal data and categories of data subjects and the obligations and rights of the controller.

As set out in Article 28 GDPR, the terms of the agreement must require that the processor:

(i) only acts on the documented instructions of the controller;
(ii) ensures the security of the personal data processed;
(iii) complies with the requirements in respect of appointing sub-processors;
(iv) implements measures to assist the controller with responding to the exercise of data subjects' rights;
(v) assists the controller in complying with its data security, breach notification and data protection impact assessment obligations;
(vi) returns or destroys the personal data at the end of the processing relationship (except as required by law); and
(vii) provides the controller with all information necessary to demonstrate compliance with the GDPR, this includes allowing for and contributing to audits.

The processor must also ensure that the persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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 rules in relation to electronic communications are set out in the e-Privacy Regulations. The principles underpinning the GDPR must also be complied with in relation to personal data processed for marketing purposes.

When email or SMS are used to send messages for direct marketing the recipient's prior opt-in consent must have been obtained. In order to rely on consent, it must be the GDPR standard of consent. There is also a soft opt-in available where an organisation is marketing its own or similar products or services to an existing customer, subject to certain requirements being met.

9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

There is also a soft opt-in for B2B emails, i.e. sending emails to an email address that reasonably appears to the sender to be an email address used mainly by the subscriber or user in the context of their commercial or official activity provided that the email relates solely to that commercial or official activity. In these circumstances, it is not necessary to obtain a recipient's prior opt-in consent.

9.3 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.).

In relation to marketing materials sent by post, recipients have the right to object at any time to the processing of their personal data for direct marketing purposes. The right to object must be brought to the attention of the recipient.

It is necessary to obtain prior consent when using automatic dialling machines to fax or send messages to an individual, or making telephone calls to an individual or non-natural person's mobile telephone for direct marketing purpose.

In respect of a body corporate, the use of automatic dialling machines, fax, email or SMS for direct marketing is permitted provided that the body corporate has not recorded its objection in the National Directory Database (the "**NDD**") or it has not opted out of receipt of direct marketing.

Telephone calls for direct marketing purposes to a subscriber or user is not permitted if the subscriber or user has recorded its objection in the NDD or has opted out of receiving direct marketing.

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

The ePrivacy Regulations are ambiguous as to whether they apply to a direct marketer based outside Ireland who sends unsolicited direct marketing communications to recipients in Ireland but it is prudent for an organisation based outside Ireland sending marketing to recipients in Ireland to assume that they do.

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

Yes, the DPC is active in this area. In its 2020 Annual Report, the DPC state that it concluded 149 electronic direct marketing investigations in 2020 and that it prosecuted six organisations for direct marketing infringements.

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

It is not unlawful to purchase marketing lists. However, organisations may only contact the individuals on such lists where those individuals have specifically consented to receipt of marketing communications and to the sharing of their personal data for those purposes (subject to the soft opt-in described at question 9.1 above).

In relation to telephone calls, the NDD (see question 9.2 above) contains information in relation to subscribers who have expressed a preference not to receive marketing calls to landline phone numbers, or have indicated consent to receiving such calls to mobile phone numbers. Organisations should check purchased marketing lists against the NDD before making any marketing telephone calls.

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

Under the e-Privacy Regulations, the penalties for sending electronic communications in breach of restrictions 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 communication that amounts to a breach constitutes an independent offence under the e-Privacy Regulations.

Where a breach of the GDPR occurs in relation to marketing communications, the organisation 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).

The e-Privacy Regulations apply to the use of cookies. Consent is required for cookies that are not strictly necessary for the service the user has explicitly requested or for the sole purpose of carrying out the transmission of a communication over an electronic communications network. The DPC released guidance on cookies in 2020. This makes clear that users must consent to cookies that are not strictly necessary before such cookies are deployed. The level of consent is the GDPR level of consent and pre-ticked boxes or sliders will not meet this standard. Users must also be provided with clear and comprehensive information in relation to cookies.

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

As outlined at question 10.1 above, consent is not required for cookies that are strictly necessary for the provision of a service explicitly requested by the user or for the sole purpose of carrying out the transmission of a communication over an electronic communications network. All other cookies must be consented to.

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

Yes. The DPC's cookies guidance was released in April 2020. The DPC granted a six-month "grace period" to website operators to ensure compliance with the guidance. Following this, the DPC investigated and commenced enforcement action against a number of website operators. The DPC's 2020 Annual Report notes that this process of cookie investigations followed by enforcement action will continue throughout 2021.

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

The penalties for breaches of applicable cookie restrictions under the 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. Each communication that amounts to a breach constitutes an independent offence under the e-Privacy Regulations.

As stated at question 9.7 above, there is a degree of overlap between the e-Privacy Regulations and the GDPR. Where a breach of the GDPR occurs in relation to cookies, an organisation 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 cannot be transferred from Ireland outside of the European Economic Area (the "EEA") unless one of the following applies:

(a) the personal data is transferred to a jurisdiction which the European Commission considers offers an adequate level of data protection;

(b) the transfer is made on the basis of the European Commission's Standard Contractual Clauses, which ensure an appropriate level of protection for the personal data. The European Commission released new Standard Contractual Clauses on 4 June 2021;

(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).

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 above.

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.

There is no requirement to notify the DPC of transfers of personal data to other jurisdictions made pursuant to Standard Contractual Clauses.

The DPC or another supervisory authority must approve BCRs which are intended to be used to transfer personal data outside the EEA within a corporate group. The DPC's 2020 Annual Report states that during 2020 the DPC continued to act or commenced acting as the lead reviewer in relation to 42 BCR applications.

11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The DPC has not released guidance following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18).

11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?

The DPC has not released guidance in relation to the European Commission's draft revised Standard Contractual Clauses or in relation to the finalised Standard Contractual Clauses that were released on 4 June 2021.

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.)?

Public and private sector employers must ensure that existing internal whistle-blower policies, and how they address whistle-blowing, meet the requirements of the Protected Disclosures Act. The concept of 'worker' under the Protected Disclosures Act includes employees, independent contractors, trainees, agency staff, and certain individuals on work experience. The Protected Disclosures Act provides an exhaustive list of relevant wrongdoings 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 recipient of a protected disclosure must not disclose any information that identifies 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.

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)?

Registration or prior approval of the use of CCTV is not required from the DPC. In respect of the use of CCTV, the GDPR must be complied with. The DPC has also released specific CCTV guidance.

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

As set out at question 13.1 above, the use of CCTV must comply with the GDPR. The DPC's CCTV guidance sets out information in respect of transparency of such processing, the lawful basis for such processing and on data protection impact assessments.

14 Employee Monitoring

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

In Ireland, there are no specific restrictions around employee monitoring. However, as monitoring involves the processing of personal data, the principles outlined at question 4.1 above must be complied with (the principles of transparency and proportionality are of particular importance).

Employees have a legitimate expectation of privacy and any monitoring and the purposes of such monitoring should be clearly set out in a policy that is made available to employees.

The DPC's guidance on CCTV states that where possible cameras should be focused on areas of particular risk, such as cash points. CCTV recording should be limited in areas where employees have an increased expectation of privacy such as changing rooms.

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

Consent is not required. However, in order to comply with transparency obligations, employees must be notified of the existence of monitoring and the purposes for which this data is processed, including if such data will be used in the context of disciplinary proceedings (this information is usually provided through an appropriate notice). The employer must have a lawful basis for the use of CCTV monitoring.

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

The extent to which works councils/trade unions/employee representatives need to be notified of such monitoring will depend on:

(i) any agreement with the relevant body;
(ii) the likelihood that the employer will seek to rely on the CCTV data; and
(iii) whether this has been covered in the relevant employee's employment contract.

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, the GDPR contains a general requirement 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.

Such measures may include:

(i) the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems and services;
(ii) the ability to restore the availability and access to personal data in a timely manner following a technical or physical incident;
(iii) pseudonymisation and encryption of personal data; 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 is made by way of a web form and must outline the nature of the personal data breach including the categories and number of data subjects concerned. The notification must also describe the likely consequences of the personal data breach, the level of risk to data subjects and outline the measures the controller proposes to adopt 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.

Under the GDPR, where a personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects, controllers must communicate it to affected data subjects without undue delay. This must describe in clear and plain language the nature of the personal data breach, include the name and contact details of the DPO (or point of contact), describe the likely consequences of the breach and outline the measures proposed to be taken or the measures that were taken by the controller to address and/or mitigate the breach.

The controller may not be required to notify the data subject(s) if the risk of harm is remote, the controller has taken measures to minimise the risk of harm or the notification requires a disproportionate effort.

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. In 2020, the DPC noted that infringements of Article 32 GDPR (security of personal data) are usually capped at a lower threshold under Article 83(4) GDPR, which could suggest that they may be less serious. However, in a number of decisions released in 2020, the DPC assessed breaches of Article 32 in light of a number of factors such as the sensitivity of the data processed and the number of personal data breaches that occurred as a result of such failure.

16 Enforcement and Sanctions

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

(a) **Investigative Powers**:
Civil/Administrative sanction – The DPC (and its authorised officers) has broad powers under the DPA to enter premises, including the right to:
(i) search and inspect a premises where processing of personal data takes place and to inspect the documents, records, statements or other information found there;
(ii) require the controller or processor or employee or agent of them to produce any documents, records, statements or other information relating to the processing of personal data, and in the case of data in a non-legible form, reproduce it in a legible form;
(iii) secure for later inspection any documents, records, data equipment including any computer, in which records may be held;
(iv) inspect, take extracts, make copies or remove and retain such documents and records as considered necessary;
(v) if a person referred to in (ii) that is required to provide a particular record is unable to provide it, require the person to state to the best of that person's knowledge where the record is located or from whom it may be obtained; and
(vi) require any person referred to in (ii) 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 undertake investigations, issue enforcement notices (which may require the controller/processor to take specific steps), require the controller/processor to provide a report on any matter and, where the DPC considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, apply to the Hight Court for an order suspending, restricting or prohibiting processing.
Criminal sanction – 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.

(b) **Corrective Powers**: The DPC has a broad 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 and to impose an administrative fine (as below).

(c) **Authorisation and Advisory Powers**: The DPC can advise the controller, accredit certification bodies and can authorise contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.

(d) **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 an organisation's worldwide annual turnover of the preceding financial year, whichever is higher.

(e) **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 an organisation's worldwide annual turnover of the preceding financial year, whichever is higher. See "Criminal sanction" in relation to "Investigative Power" above.

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 DPC can issue an order on a particular processing activity, including a ban on processing. Such a ban does not require a court order.

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

The DPC regularly enforces its powers. In its 2020 Annual Report, the DPC stated that on 31 December 2021 it had 83 statutory inquiries on hand, including 27 cross-border inquiries. These inquiries are a mixture of own-volition inquiries as well as being complaint-based. In 2020, the DPC released a number of decisions. In December 2020, the DPC issued its first fine in a cross-border case.

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

Under the GDPR, the DPC can enforce against organisations established in other jurisdictions where such organisations come within the scope of the GDPR. The DPC can enforce its powers through an organisation's GDPR representative.

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?

Requests from international authorities are typically made pursuant to mutual legal assistance treaties. The Criminal

Justice (Mutual Assistance) Act 2008 sets out how Ireland engages with other countries in respect of law enforcement requests on foot of various treaties and conventions, with the aim of streamlining requests between different authorities and ensuring that adequate safeguards are in place to protect individuals. The Minister for Justice and Equality acts as the "Central Authority" for mutual assistance, confirming the validity of requests for assistance and checking that the provisions of the Criminal Justice (Mutual Assistance) Act 2008 are satisfied.

Organisations may receive direct requests from authorities outside of the mutual legal assistance process. There is more risk associated with handling such requests, such that organisations will often prefer to refer the requester to the mutual legal assistance process where they have no legal obligation to produce the records that have been requested.

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

To date, the DPC has issued limited guidance in this area. This set out information in relation to the Law Enforcement Directive and guidance in relation to how an organisation should determine whether a matter is within the scope of the directive.

18 Trends and Developments

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

The DPC released a number of decisions in 2020. The majority of these stemmed from investigations that were initiated in response to personal data breaches. The DPC issued its first fine in a cross-border case, fining Twitter International Company €450,000. The DPC's decisions contained a variety of enforcement measures including fines, orders to bring data processing into compliance and reprimands. In December 2020, the DPC had 83 statutory inquiries ongoing and it is expected that the DPC will issue a number of decisions in 2021.

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

The processing of children's data. The DPC issued its draft Fundamentals for a Child-Oriented Approach to Data Processing (the "**Fundamentals**") in December 2020 which were open for consultation until 31 March 2021. It is expected that the DPC will issue its final version of the Fundamentals in 2021. The DPC is also expected to work with the industry to produce sectoral codes in relation to the processing of children's data.

Cookies were a special project of the DPC in 2020. In early 2020, the DPC conducted a "regulatory sweep" of some of the frequently visited websites in Ireland to establish levels of compliance with the e-Privacy Regulations. Following the completion of the sweep, the DPC produced specific and detailed cookies guidance. The DPC also investigated and commenced enforcement action against a number of website operators. The DPC has noted that the process of cookies investigations followed by enforcement action will continue throughout 2021.

Colin Rooney is partner in the Technology and Innovation Group of Arthur Cox in Dublin. His practice focuses on technology matters, with a particular focus on data privacy and data security and covers a broad range of work, ranging from regulatory dealings and negotiations, to compliance and counselling. His practice also has a strong emphasis on commercial IT agreements.

Arthur Cox LLP
Ten Earlsfort Terrace
Dublin 2
Ireland

Tel: +353 1 920 1194
Email: colin.rooney@arthurcox.com
URL: www.arthurcox.com

Aoife Coll is an associate on the Technology & Innovation team at Arthur Cox. Aoife regularly advises a broad range of clients including private sector, public sector and non-profit bodies on a variety of matters. Aoife advises on compliance with data protection laws, including GDPR compliance as well as on technology matters more generally.

Arthur Cox LLP
Ten Earlsfort Terrace
Dublin 2
Ireland

Tel: +353 1 920 1726
Email: aoife.coll@arthurcox.com
URL: www.arthurcox.com

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group