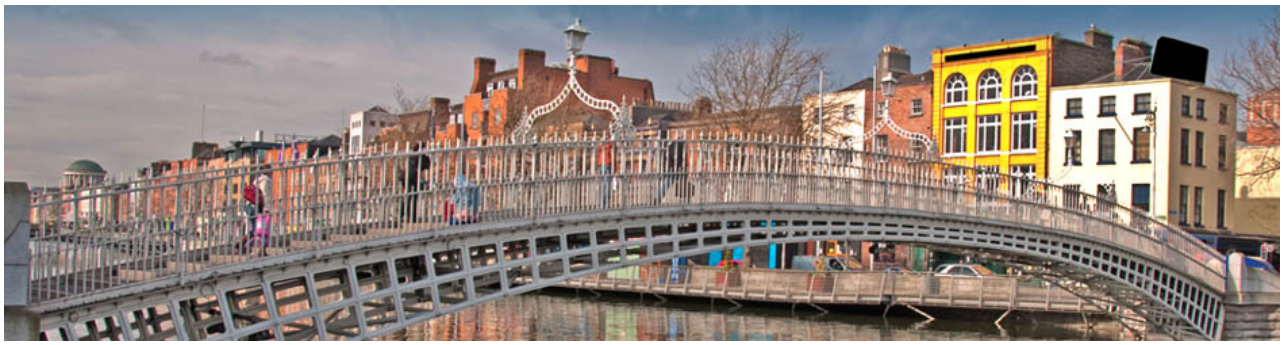
DATA PROTECTION LAWS OF THE WORLD

Ireland

DLA PIPER

IRELAND



Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Irish Data Protection Act 2018 (“**DP Act**”) came into force on 25 May 2018 in order to give further effect to the GDPR in Ireland. The DP Act includes certain derogations, provides for the establishment of a new Data Protection Commission, implements the Law Enforcement Directive and otherwise addresses procedural aspects of the enforcement of data protection in Ireland.

The previous data protection legislation in Ireland, the Data Protection Acts 1988 to 2003, were largely repealed by the DP Act, however those Acts continue to apply in relation to certain limited purposes including national security and defence. Additionally, the previous legislation continues to apply in relation to complaints or infringements which occurred prior to 25 May 2018 as well as to investigations commenced (but not completed) prior to that date.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number,

phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are terms used in the GDPR. For the purposes of the DP Act, the definition of a “**public body**” includes a company (and its subsidiaries) in which the majority of shares are held by or on behalf of a Minister of the Government.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The DP Act established the Data Protection Commission (“**DPC**") to act as the supervisory authority for data protection law in Ireland.

As well as supervising many domestic Irish businesses and organisations, the DPC also regulates many international and multi-national companies under the GDPR’s main establishment (or “one-stop shop”) regulatory mechanism.

Ireland has had one acting Commissioner for Data Protection, Helen Dixon, who served two five-year terms. However, the DP Act provides that the DPC can consist of up to three members. The Government, during July 2022 approved the commencement of the process to appoint two additional Commissioners. It is expected that at least two Commissioners

will be appointed from 2024 onwards. In the event that there is more than one Commissioner, one of the Commissioners will be appointed as Chairperson.

The contact details of the DPC (or *An Coimisiún um Chosaint Sonraí*) are as follows:

Dublin office

21 Fitzwilliam Square South
Dublin 2, D02 RD28
Ireland

Regional office

Canal House
Station Road
Portarlington
R32 AP23 Co. Laois
Ireland

Website

www.dataprotection.ie

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no general requirement in Ireland for controllers or processors to register their processing activities with the DPC, however, a register of Data Protection Officers (DPOs) is maintained.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities

(Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Ireland has not yet extended the requirement to appoint a Data Protection Officer (“**DPO**”). However, Section 34 of the DP Act does provide the Minister for Justice and Equality with the power to make regulations requiring controllers or processors to designate a data protection officer.

In addition, the DP Act requires enhanced “suitable and specific” measures to be implemented in relation to certain processing activities. In such cases, the designation of a DPO (in cases where it is not mandatory under GDPR) is listed in section 36 of the DP Act as one example of such measures.

The DPC maintains a register of DPOs. No fee is charged for registering or updating the details of a DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known as lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was

not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information

about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. necessary for entering into or performing a contract;
2. authorized by EU or Member State law; or
3. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Part 3 of the DP Act sets out a range of national derogations as provided for in GDPR. Some of the notable provision include the following.

Processing for purpose other than purpose for which data collected

Section 41 of the DP Act permits the processing of personal data or special categories of personal data for purposes other than for which it was collected where necessary and proportionate for the purposes of: (a) preventing threats to national security, defence or public security; (b) preventing detecting, investigating or prosecuting crime; (c) providing / obtaining legal advice; (d) in connection with legal claims or prospective claims; or (e) establishing, exercising or defending legal rights.

Special category data

Chapter 2 of Part 3 governs the processing of special category personal data. The DP Act permits the processing of special category in certain circumstances including:

- for employment / social welfare law purposes;
- in relation to legal advice and proceedings;
- in the course of electoral activities;
- for the purposes of the administration of justice;
- for certain insurance or pension purposes as well as in relation to the mortgaging of a property;
- for reasons of substantial public interest;
- by health care workers for medical, health and social care purposes;
- in the interests of public health; and
- for archiving, scientific, historic or statistical purposes.

In most such cases, the DP Act requires enhanced “suitable and specific” measures to be implemented in order to protect the rights and freedoms of data subjects. The DPC has the right to request evidence of such measures, which can include:

- explicit consent of the data subject;
- limitations on access to the personal data;
- strict time limits for erasure of the personal data;
- specific training for those processing the personal data;
- various enhanced technical and organisational measures such as encryption and pseudonymisation; and
- processes and procedures for risk assessment purposes.

Health research regulations

The Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 came into force in August 2018. The Health Research Regulations introduced material changes to the rules governing how health research can be conducted in Ireland and include:

- a new statutory definition of “health research”;
- a prescribed list of mandatory “suitable and specific measures” that must be adopted when processing personal data for health research purposes, including a general requirement that “explicit consent” be obtained from data subjects; and
- a list of exceptional circumstances in which the explicit consent requirement is not required and a detailed process to be followed in such cases.

Article 10 (criminal records) data

The DP Act expands the definition of Article 10 data to include personal data relating to the alleged commission of an offence and any proceedings relating to such offence. Section 55 of the DP Act provides for Article 10 (i.e. criminal records) data to be lawfully processed in a number of limited circumstances including:

- where the data subject has given explicit consent;
- where necessary and proportionate for the performance of a contract to which the data subject is party;
- where necessary for providing / obtaining legal advice or in connection with legal claims or prospective claims;

- where necessary for establishing, exercising or defending legal rights; or
- where necessary to prevent injury or damage or otherwise to protect vital interests.

The DP Act also requires enhanced “suitable and specific” measures to be taken to safeguard the rights and freedoms of data subjects in all of the above circumstances.

Children & child's consent to information society services

The DP Act defines a "child" as a person under 18 (this is relevant for example in assessing whether or not a data protection impact assessment may be required).

The DP Act provides that the digital age of consent in Ireland is 16 years old. This means that in order for any personal data pertaining to a child below the age of 16 to be processed in relation to an information society service, the consent of a parent or guardian is also required. The DPC ran two public consultations in 2019 on the processing of children’s personal data and the rights of children as data subjects and published the “Fundamentals for a Child-Oriented Approach to Data Processing” in December 2021. The DPC also has a statutory function, under section 32 of the DP Act, to encourage the drawing up of codes of conduct for the protection of children.

Section 33 of the DP Act provides a specific right of erasure for children in connection with personal data collected in relation to the offer of information society services.

The DP Act includes a prohibition on the processing of children's personal data for the purposes of direct marketing, profiling and micro-targeting. Section 30 has however not been commenced due to concerns that enacting it would place Ireland in breach of EU law.

Automated decision making

Section 57 of the DP Act provides for a derogation whereby the right under GDPR not to be subject to a decision based solely on automated decision-making including profiling where the decision is authorised or required under an enactment and either (1) the effect of the decision is to grant a request of the data subject, or (2) adequate steps have been taken to safeguard the legitimate interests of the data subject.

Rights of data subjects

Section 60 of the DP Act sets out the circumstances in which data subject rights may be restricted. These include where such restrictions are necessary and proportionate:

- to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State;
- for the prevention, detection, investigation and prosecution of criminal offences;
- for the administration of taxes or duties;
- for the establishment, exercise or defence of, a legal claim or prospective legal claim;
- for the enforcement of civil law claims; or
- for the purposes of estimating the amount of the liability of a controller on foot of a claim.

Section 60 also restricts data subject rights to the extent that the personal data relating to the data subject is an expression or opinion by another person given in confidence, or on the understanding that it would be treated as confidential. The person in receipt of the information must have a legitimate interest in receiving the information.

Data subject rights can also be restricted in relation to information which is subject to legal privilege.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and

Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, South Korea, United Kingdom, Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others: binding corporate rules, standard contractual clauses and the EU-US Privacy Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

1. explicit informed consent has been obtained;
2. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
4. the transfer is necessary for important reasons of public interest;
5. the transfer is necessary for the establishment, exercise or defence of legal claims;
6. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
7. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Section 37 of the DP Act provides the Minister for Justice and Equality with the power to make regulations restricting the transfer of categories of personal data to a third country or an international organisation for important reasons of public policy.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

1. the pseudonymization and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The DP Act requires enhanced “suitable and specific” measures to be implemented in relation to certain processing activities. In such cases, enhanced data security measures (including logs / audit trails and encryption) are listed in section 36 of the DP Act as one example of such measures.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*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*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to the DPC which has a published web form and risk rating requirement for personal data breach notifications.

The online breach reporting web form requires specific information to be provided depending on whether the personal data breach is a national or cross-border breach (in the latter case where the DPC acts as the lead supervisory authority under GDPR’s main establishment (or “one-stop shop”) regulatory mechanism). Further specific information is required to be provided for telecommunications and internet service providers to report breaches under Commission Regulation (EU) No 611/2013.

Organisations reporting breaches are requested to provide a self-declared risk rating using the following thresholds:

- *Low Risk*: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- *Medium Risk*: The breach may have an impact on individuals, but the impact is unlikely to be substantial.
- *High Risk*: The breach may have a considerable impact on affected individuals.
- *Severe Risk*: The breach may have a critical, extensive or dangerous impact on affected individuals.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf

(Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Enforcement powers

Part 6 of the DP Act provides the DPC with a wide-range of powers to supervise organisations under its jurisdiction, including:

- Powers to handle complaints made (directly or indirectly) to it;
- Powers to open and conduct “own-volition” inquiries;
- Powers to issue decisions and exercise corrective powers (including administrative fines) provided for in GDPR;
- Powers to issue a variety of corrective orders including warnings, reprimands, directions, suspensions or restrictions;
- Powers of entry, search, seizure and inspection, including the removal and retention of documents or records;
- Powers to issue information and enforcement notices; and
- Powers to require an organisation to carry out a report or audit.

Criminal offences

The DP Act provides for several offences which can result in prosecution, imprisonment, and criminal penalties being imposed. Where offences are committed by an organisation, and such offence is committed with the consent, connivance or negligence of a manager, director, secretary or other officer of the company, the individual will be personally liable for the offence, as well as the organisation. The offences under the DP Act include:

- an employer or potential employer forcing an individual to make a subject access request;
- a processor disclosing personal data without the consent of the controller unless required to do so by law;
- obtaining and disclosing, or selling personal data to a third party without the consent of the relevant controller or processor of that data, or in relation to data which were unlawfully disclosed to them;
- contravening the provisions relating to the processing of criminal convictions and offences data;
- not cooperating with an authorised officer during an investigation, audit or inspection; and
- failing to comply with an information or enforcement notice.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be

replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The ePrivacy Regulations implement the anti-spam rules set out in Article 13 of the Privacy and Electronic Communications Directive 2002/58/EC (as amended by the Citizens’ Rights Directive). These regulations came into effect on 1 July 2011. Electronic mail includes text messages (SMS), voice messages, sound messages, image messages, multimedia message (MMS) and email messages.

Direct marketing emails can generally only be sent to users with their prior consent. A limited exemption is available for direct marketing emails sent to existing customers promoting other products or services similar to those previously purchased by that consumer (such emails can only be sent for 12 months, the customer must have been given the opportunity to object when the details were collected and the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer). B2B direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages.

The identity of the sender must not be disguised or concealed and the recipient must be offered an opt-out.

Direct marketing calls (excluding automated calls) may be made to a landline provided the subscriber has not previously objected to receiving such calls or noted his or her preference not to receive direct marketing calls in the National Directory Database.

Direct marketing calls cannot be made to a mobile phone without prior consent.

One cannot send a direct marketing fax to an individual subscriber in the absence of prior consent. One can send such a fax to a corporate subscriber unless that subscriber has previously instructed the sender that it does not wish to receive such communications or has recorded a general opt-out to receiving such direct marketing faxes in the National Directory Database.

Breach of these anti-spam rules is a criminal offence. On a summary prosecution (before a judge sitting alone) a maximum fine of EUR 5,000 per message sent can be handed down. On conviction on indictment (before a judge and jury) a company may be fined up to EUR 250,000 per message sent and an individual may be fined up to EUR 50,000 per message.

The GDPR applies to most electronic marketing activities, as these will typically involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47 of GDPR). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (“**ePrivacy Directive**”), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation though there remains uncertainty at an EU level as to when this legislation will be passed. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In Ireland, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic

Communications) Regulations 2011 (“**ePrivacy Regulations**”) implement the rules on electronic direct marketing set out in the ePrivacy Directive.

Direct marketing emails (which includes SMS and other text, voice, sound or image messages) can generally only be sent to users with their prior (opt-in) consent.

Two exemptions are available whereby emails can be sent on an opt-out basis:

Customer exception

Direct marketing emails may be sent on an opt-out basis to an existing customer promoting similar products or services to those purchased by that customer. Such emails can only be sent for 12 months from the date of sale to the customer, the customer must be given the opportunity to object both (1) when the details were collected, and (2) in each marketing message. Moreover, the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer.

B2B exception

Business to business (**"B2B"**) direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages. To qualify for the B2B exception, an email address must reasonably appear to the sender to be an email address used mainly by the recipient in the context of their commercial or official activity and the marketing message must relate solely to that commercial or official activity.

ONLINE PRIVACY

Cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. A user must be provided with ‘clear and comprehensive information’ about the cookie (including, in particular, its purposes). This information must be prominently displayed and easily accessible. The methods adopted for giving information and obtaining consent should be as ‘user friendly’ as possible. The DPC has provided regulatory guidance on cookies and other tracking technologies which can be accessed here.

Location Data

One cannot process location data unless either:

- such data has been made anonymous; or
- user consent has been obtained.

A provider of electronic communication networks or services or associated facilities (i.e. a telco) must inform its users of:

- the type of location data (other than traffic data) that will be processed;
- the purpose and duration of the processing; and
- whether the data will be transmitted to a third party to provide a value added service. Users can withdraw their consent to the processing of location data.

Cookies

The use of cookies (and similar technologies) is regulated by the GDPR as well as the ePrivacy Regulations.

The ePrivacy Regulations provide that a person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless (1) the subscriber

or user has given his or her consent to that use, and (2) the subscriber or user has been provided with clear and comprehensive information which (a) is both prominently displayed and easily accessible, and (b) includes, without limitation, the purposes of the processing of the information.

The DPC’s guidance has confirmed that all cookies and tracking technology tools require consent, apart from two exceptions:

- **Communications exemption** – a cookie whose sole purpose is to carry out the transmission of a communication over a network; and
- **Strictly necessary exemption** – this applies to a service delivered over the internet (e.g. websites or apps) which have been explicitly requested by the user and the use of cookies is restricted to what is strictly necessary to provide that service.

The DPC commenced enforcement action on compliance with its regulatory guidance for controllers in October 2020.

Location data

The ePrivacy Regulations deal with the collection and use of location and traffic data by electronic communications network and service providers. Location data other than traffic data relating to users or subscribers of undertakings can only be processed if (1) such data are made anonymous, or (2) the consent of the users or subscribers has been obtained to the extent and for the duration necessary for the provision of a value added service.

KEY CONTACTS

John Magee
Partner
T +353 1 436 5450
john.magee@dlapiper.com

Eilis McDonald
Senior Associate
T +353 1 436 5479
eilis.mcdonald@dlapiper.com

Sarah Dunne
Associate
T +353 14 876699
sarah.dunne@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.