DATA PROTECTION & PRIVACY

Ireland

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 05 August 2022

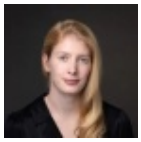
Table of contents

Contributors

Ireland

Shane Martin
shane.martin@walkersglobal.com
Walkers

Conor Daly
conor.daly@walkersglobal.com
Walkers



Coleen Wegmann
coleen.wegmann@walkersglobal.com
Walkers

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Since 25 May 2018, the key legislative instrument applicable in Ireland for the protection of PI has been the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The Irish Data Protection Acts 1988 to 2018 (DPA) supplement and give further effect to the GDPR. Data protection is a fundamental right set out in article 8 of the EU Charter of Fundamental Rights and Irish courts have also recognised the right to privacy as one of the unenumerated rights recognised by the Irish constitution.

The legislative framework for the protection of PI also includes the Law Enforcement Directive (Directive (EU) 2016/680) in the context of criminal investigations and prosecutions. The Law Enforcement Directive is transposed into Irish law by the DPA.

The final key element of the legislative framework in Ireland is the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the Irish ePrivacy Regulations), which transpose the Privacy and Electronic Communications Directive 2002 (the ePrivacy Directive) into Irish law.

Law stated - 24 May 2022

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Data Protection Commission (DPC) is the independent data protection supervisory authority in Ireland with responsibility for the enforcement of the GDPR and safeguarding the fundamental right of individuals in the European Union to the protection of their PI. The DPC also has powers and responsibilities relating to the Irish ePrivacy Regulations and the Law Enforcement Directive.

The DPC's investigative powers include the power to:

- conduct investigations on compliance with the GDPR, including in the form of data protection audits and, where necessary, take enforcement action;
- investigate complaints received from individuals regarding potential infringements of data protection law;
- order individuals and organisations involved in the processing of PI to provide any information it requires for the performance of its tasks;
- carry out a review of data protection certifications issued by it pursuant to the GDPR;
- notify the controller or the processor of an alleged infringement of the GDPR; and
- obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with all applicable laws.

Law stated - 24 May 2022

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

As an EU data protection supervisory authority, the DPC is represented on the European Data Protection Board (EDPB). The EDPB works to ensure the consistent application of the GDPR across the European Union.

Under the GDPR, the DPC cooperates and collaborates with other data protection authorities on matters of legal interpretation and on specific cases through its participation in the 'one-stop-shop' mechanism. Under this mechanism, organisations that have their main establishment in an EU member state may elect to be primarily regulated by the supervisory authority of the jurisdiction in which their main establishment is located.

As part of the one-stop-shop mechanism, the DPC provides and receives mutual assistance to and from other concerned supervisory authorities and conducts joint investigations and joint enforcement actions with other concerned supervisory authorities.

Law stated - 24 May 2022

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

If the DPC finds that a breach of applicable data protection law has occurred, it may employ a number of different corrective powers. These corrective powers include facilitating amicable resolution of the matter, issuing a warning or reprimand to an organisation, issuing an order to bring data processing operations into compliance with the GDPR, imposing a temporary or permanent processing limitation on an organisation and imposing an administrative fine.

An administrative fine levied against an organisation for an infringement may be set at up to €20 million or 4 per cent of the organisation's total worldwide annual turnover for the preceding financial year (whichever figure is higher).

According to the GDPR, when deciding to impose an administrative fine on an organisation, the DPC must give due regard to a number of factors, including:

- the nature, gravity and duration of the infringement, as well as the number of individuals affected and the level of damage they have suffered;
- the intentional or negligent character of the infringement;
- any actions taken by the organisation to mitigate the damage;
- any previous infringements by the organisation;
- the categories of PI involved; and
- the manner in which the DPC has become aware of the infringement.

In addition to administrative sanctions, certain PI breaches can also lead to criminal sanctions. For example, the following breaches may constitute criminal offences:

- disclosure of a person's PI by a controller or processor, without prior authority;
- processing the PI of a child for the purposes of direct marketing, profiling or micro-targeting;
- obstructing an authorised officer of the DPC in the performance of his or her functions; and

- failing to comply with a requirement specified in a DPC enforcement notice.

Summary proceedings for an offence under the DPA may be brought and prosecuted by the DPC. Criminal penalties can include fines of up to €250,000, imprisonment for up to five years or both.

Law stated - 24 May 2022

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

PI owners have the right to appeal to the courts against orders of the DPC.

Law stated - 24 May 2022

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

While no particular sectors or types of organisation are exempt from the scope of the General Data Protection Regulation (GDPR) and the Irish Data Protection Acts 1988 to 2018 (DPA), some specific exemptions exist.

The GDPR states that the processing of PI by individuals for purely personal and domestic use are outside the scope of the GDPR.

The GDPR and the DPA also apply to public sector bodies. However, processing of PI by competent authorities for law enforcement purposes is outside the scope of the GDPR. Processing of PI for this purpose is subject to rules in Part 5 of the DPA.

Law stated - 24 May 2022

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Irish ePrivacy Regulations protect the confidentiality of electronic communications and also contain requirements relating to electronic marketing. Where electronic communications involve the processing of PI by organisations, the GDPR and the DPA will also apply.

The Postal Packets and Telecommunications (Regulation) Act 1993 provides a legislative basis for the lawful interception and covert surveillance in the context of the fight against organised crime and terrorism. The Irish government published proposals in 2020 to update the legislative framework in this area.

Law stated - 24 May 2022

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

There are a number of statutory instruments that provide specific data protection rules in the areas of health and social work, including:

- SI Number 18/2021 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021;
- SI Number 82/1989 – Data Protection (Access Modification) (Health) Regulations 1989; and
- SI Number 83/1989 – Data Protection (Access Modification) (Social Work) Regulations 1989.

The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018, which implemented the EU Directive on the Security of Network and Information Systems, imposes information security standards and incident reporting-related obligations on digital service providers.

Outside the general principles provided for by the GDPR and the DPA, there is no specific legislation in Ireland governing the monitoring of employees. However, the right to privacy of a worker must be balanced against the right of an employer to protect its business interests. Any monitoring of employees by an employer in the workplace must be necessary, legitimate and proportionate, and such monitoring must be clearly communicated in the employer's privacy notice.

There is no specific legislation governing the use of social media by employees, however it is recommended that employers should have a clear policy on the acceptable use of social media in the workplace. Any monitoring of employees' social media use should be notified to employees and the purpose of such monitoring should be explained in the relevant policy or privacy notice. Profile screening of social media in recruitment and during employment can give rise to claims of discrimination and breach of privacy and data protection laws. Pre-hire criminal background checks are not permitted except where the role involves services being provided to children or vulnerable adults or work in the security industry.

Law stated - 24 May 2022

PI formats

What categories and types of PI are covered by the law?

The GDPR and the DPA apply to all forms of PI in electronic form and PI in manual form provided the latter forms part of, or is intended to form part of, a 'filing system'.

Law stated - 24 May 2022

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR applies to organisations established in any EU member state, including Ireland, where the organisation engages in the processing of PI of individuals. The GDPR will also apply to EU-based organisations where the

processing of the PI takes place outside the European Union.

The GDPR also states that organisations established outside the European Union will be subject to the GDPR where they process the PI of individuals located in an EU member state (the targeted individuals) in connection with offering goods or services to such data subjects or in connection with monitoring the behaviour of such data subjects. Controllers or processors that come within the scope of the GDPR in this way must designate a representative in an EU member state where the targeted individuals are located.

Law stated - 24 May 2022

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR contains a broad definition of processing such that virtually all processing and uses of PI by a controller or processor will be covered by the GDPR.

The GDPR identifies a controller as the party that, alone or jointly with others, determines the purposes and means of the processing of PI. The GDPR defines a processor as an individual or organisation that processes PI on behalf of a controller. The GDPR also notes that a processor must not process PI except on the instructions of the controller.

Both controllers and processors have certain duties and responsibilities in relation to the appropriate and secure processing of PI under the GDPR. However, the controller is the primary decision maker and has primary responsibility in relation to the PI.

Law stated - 24 May 2022

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The GDPR states that the processing of PI will only be lawful when one or more of the following lawful bases apply to the processing of the PI:

- the data subject has given prior, freely given and informed consent to the processing of his or her PI for one or more specific purposes. Importantly, consent should not be relied upon as a legal basis where there is a clear imbalance of power between the data subject and the controller;
- processing is 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;
- processing is necessary for compliance with a legal obligation (not including contractual obligations or obligations arising under the law of a non-EU jurisdiction) to which the controller is subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest; and
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Law stated - 24 May 2022

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

The GDPR provides for a number of specific requirements for the lawful processing of sensitive PI (also known as 'special categories of PI'). The GDPR describes sensitive PI as including PI revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health; and
- data concerning a natural person's sex life or sexual orientation.

To lawfully process sensitive PI in accordance with the GDPR, the controller must establish that: (1) one of the lawful bases for processing non-sensitive PI applies to the processing of the PI; and (2) one of the additional grounds for processing sensitive PI as set out in the GDPR applies to the processing of the sensitive PI.

The additional grounds for the lawful processing of sensitive PI according to the GDPR include the following:

- the data subject has given prior explicit, freely given, informed consent to the processing of their sensitive PI for one or more specified purposes;
- processing is necessary in the context of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the PI is not disclosed outside that body without the consent of the data subjects;
- processing relates to PI that is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of EU or EU member state law; and
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or EU member state law.

The Irish Data Protection Acts 1988 to 2018 (the DPA) also include some additional grounds that may provide a legal basis for the processing of sensitive PI. These include processing sensitive PI for the following purposes as further defined in the DPA:

- employment and social welfare law;

- legal advice and legal proceedings;
- by the Irish Referendum Commission in connection with the electoral activities;
- the administration of justice;
- insurance and pension purposes;
- substantial public interest; and
- public health.

Law stated - 24 May 2022

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Pursuant to the General Data Protection Regulation (GDPR), controllers must adhere to the principle of transparency when processing PI and are required to provide certain information to the data subject at the time the PI is collected. To comply with these requirements, controllers typically provide data subjects with a data privacy notice containing the following mandatory information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the controller's data protection officer, where applicable;
- the purposes of the processing for which the PI are intended as well as the legal basis for the processing;
- the recipients or categories of recipients of the PI, if any;
- where applicable, the fact that the controller intends to transfer PI to a third country and details of the safeguarding mechanism to be relied upon to ensure the security of the PI being transferred;
- the period for which the PI will be stored;
- the existence of the right of the data subject to request from the controller access to and rectification or erasure of or restriction of processing of their PI or to object to the processing of their PI, as well as their right to data portability;
- where the legal basis for processing is the data subject's consent, the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with the Data Protection Commission or another relevant EU data protection supervisory authority;
- whether the provision of PI is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the PI and of the possible consequences of failure to provide such data; and
- the existence of automated decision-making, including profiling, including the significance and the envisaged consequences of such processing for the data subject.

If the controller wishes to further process a data subject's PI for a new purpose after it has been collected, the controller must provide the data subject with information on that other purpose prior to that further processing.

Where PI has not been obtained directly from the data subject, the controller must provide the data subject with a privacy notice:

- within a reasonable period after obtaining the PI, but at the latest within one month;
- if the PI is to be used for communication with the data subject, at the latest at the time of the first communication

to that data subject; or
- if the PI is to be disclosed to another party, the notice should be provided when the PI is first disclosed, at the latest.

Law stated - 24 May 2022

Exemptions from transparency obligations

When is notice not required?

It is not necessary to provide a privacy notice where:

- the data subject already has the information that would be included in the privacy notice;
- the provision of the privacy notice would be impossible or would involve a disproportionate effort (in such cases the controller must take appropriate measures to protect the data subject's rights and freedoms, including making the information publicly available);
- obtaining or disclosing the PI is expressly provided for under EU or EU member state law to which the controller is subject and that law provides appropriate measures to protect the data subject's legitimate interests; or
- where the PI is subject to an obligation of professional secrecy regulated by EU or EU member state law.

Law stated - 24 May 2022

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

Controllers and processors engaging in the processing of PI must abide by the principles relating to the processing of PI. One of the principles relating to the processing of PI is that PI must be accurate and, where necessary, kept up to date.

Law stated - 24 May 2022

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

Controllers and processors engaging in the processing of PI must comply with the data processing principle of ensuring the PI they process is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (known as the principle of data minimisation).

Law stated - 24 May 2022

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Controllers and processors engaging in the processing of PI must comply with the principle of data minimisation.

PI must be held in a form that permits identification of data subjects only for as long as is necessary for the purposes for which the PI is processed (known as the principle of storage limitation).

There are no specific limits set out in the GDPR or the DPA to be complied with to satisfy the principles of data minimisation or storage limitation. However, time limits for the retention of records containing PI may be specified in other legislation such as anti-money laundering legislation.

Law stated - 24 May 2022

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The GDPR provides that PI may only be processed for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. This principle is known as purpose limitation.

The processing of PI for purposes other than those for which the PI was initially collected is only permitted where the further processing is compatible with the purposes for which the PI was initially collected. In such a case, notice of the new purposes must be provided to the data subject. Where the new purposes would be incompatible with the original purposes, the consent of the data subject will be required unless an exemption applies.

Law stated - 24 May 2022

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

An individual has the right to not be subject to automated decisions without human intervention that affect them. Such automated decision-making is permitted only with the express consent of the individual, when necessary for the performance of a contract or when authorised by EU or member state law. Where one of these exceptions applies, suitable measures must be in place to safeguard the individual's rights, freedoms and legitimate interests. Where automated processing relates to special categories of personal data, processing is only lawful where the individual has given express consent to the processing, or where it is necessary for reasons of substantial public interest.

Law stated - 24 May 2022

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The General Data Protection Regulation (GDPR) imposes a general obligation on owners of PI (controllers) and service providers that process PI on their behalf (processors) to ensure the security of data subjects' PI by implementing 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk'. The measures that an organisation chooses to implement must be assessed in the context of 'the nature, scope, context and purposes of processing' together with the risk and potential impact of a data security breach on the rights and freedoms of natural persons.

The GDPR provides examples of steps that controllers and processors may use to secure the PI for which they are responsible including:

- the pseudonymisation and encryption of PI; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

When appointing a processor, a controller must ensure that the contract appointing the processor requires the processor to employ all necessary security measures to ensure compliance with the GDPR.

Law stated - 24 May 2022

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Pursuant to the GDPR, controllers are required to notify the Data Protection Commission (DPC) of a data breach without undue delay, and no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

The GDPR also requires controllers to notify a data breach to the affected individuals without undue delay where the PI breach is likely to result in a high risk to the rights and freedoms of the affected individuals. In circumstances where a controller has not communicated a data breach to the affected individuals, the DPC may require the controller to notify the affected individuals based on its assessment of whether the data breach would be likely to result in a high risk.

Processors are required to notify the relevant controller of a data breach without undue delay.

Law stated - 24 May 2022

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The General Data Protection Regulation (GDPR) integrates accountability as a key principle that requires that owners of PI put in place appropriate technical and organisational measures to be able to demonstrate what they did and its effectiveness, when requested.

Law stated - 24 May 2022

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer (DPO) is required where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing sensitive PI or PI relating to criminal offences and convictions on a large scale.

Organisations may also elect to appoint a DPO voluntarily, although such an appointment will need to comply with the requirements of the General Data Protection Regulation (GDPR). The DPO's appointment is required to be notified to the DPC, and the DPC has issued guidance on the experience and qualifications that a DPO should have to undertake the role. The guidance confirms that a DPO's level of qualification and experience should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed.

A DPO is required by the GDPR to:

- inform and advise the controller or the processor and its employees of their obligations pursuant to the GDPR and other requirements of EU or EU member state data protection law;
- monitor compliance with the GDPR and with the policies of the controller or processor in relation to the protection of PI, awareness-raising, staff training and audits;
- provide advice where requested as regards any data protection impact assessment (DPIA) undertaken and monitor the performance of the DPIA; and
- cooperate with the supervisory authority and act as the contact point for the supervisory authority on issues relating to processing.

Law stated - 24 May 2022

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Controllers and processors of PI are required to maintain internal written records of all processing activities for which they are responsible.

In particular, the GDPR stipulates that a controller should record:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the controller's DPO;
- the purposes of the particular processing activity;
- a description of the categories of data subjects and of the categories of PI that are processed;
- the categories of recipients to whom the PI have been or will be disclosed;
- details of any transfers of PI to a third country or an international organisation, including the suitable safeguards employed in respect of the transfers;
- the time limits for retention of the PI being processed; and
- a general description of the technical and organisation security measures implemented in respect of the PI.

The GDPR also states that a processor must maintain a record of all processing activities undertaken on behalf of a controller, including:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the DPO;
- the categories of processing carried out on behalf of each controller;
- where applicable, details of transfers of PI to a third country or an international organisation, including the suitable safeguards employed in respect of the transfers; and
- where possible, a general description of the technical and organisational security measures implemented in respect of PI.

The obligations relating to record-keeping do not apply in circumstances where an organisation employs fewer than 250 persons. However, this exemption does not apply where the processing is likely to result in a risk to the rights and freedoms of data subjects, processing is not occasional or the PI being processed includes sensitive PI.

Law stated - 24 May 2022

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The GDPR requires that a controller carry out an advance assessment of the impact of envisaged processing operations on the protection of PI (known as a data protection impact assessment (DPIA)) where processing includes the use of new technologies and is likely to result in a high risk to the rights and freedoms of natural persons.

In particular, the GDPR provides that a DPIA will be required in the case of:

- automated processing, including profiling;
- processing on a large scale of sensitive PI or PI relating to criminal offences and convictions on a large scale; and
- large scale systematic monitoring of a publicly accessible area.

Pursuant to the GDPR, the DPIA must at least contain:

- a systematic description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of PI and to demonstrate compliance with the GDPR.

Law stated - 24 May 2022

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The GPDR requires controllers to ensure ‘data protection by design’ and ‘data protection by default’. Data protection by

design means embedding data privacy features into the design of projects at an early stage. Data protection by default means that the user service settings must be automatically data protection-friendly, and that only data necessary for each specific processing purpose should be gathered.

Law stated - 24 May 2022

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no requirement for controllers or processors to register with the Data Protection Commission in relation to the data processing activities that they undertake.

Law stated - 24 May 2022

Other transparency duties

Are there any other public transparency duties?

A controller or processor that appoints a data protection officer (DPO) must publish the contact details of the DPO.

Law stated - 24 May 2022

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

When appointing a service provider to provide data processing services, a controller must only use a processor that provide sufficient guarantees to implement appropriate security measures to meet the requirements of the General Data Protection Regulation (GDPR) and ensure the protection of the rights of the data subjects.

Controllers are also required to put in place a written contract with a processor containing a number of provisions as set out in the GDPR that require the processor to:

- act only on the documented instructions from the controller;
- ensure that persons that will process PI are subject to an obligation to keep the PI confidential;
- take all security measures required by the GDPR;
- obtain prior specific or general written authorisation of the controller before appointing any sub-processors and ensure that sub-processors are subject to obligations equivalent to those imposed on the processor;
- assist the controller insofar as possible to comply with the controller's obligation to respond to data subjects' rights requests;
- assist the controller in ensuring compliance with its obligations regarding notification of PI breaches to the supervisory authority and data subjects (where necessary) and to carry out data protection impact assessments;
- at the choice of the controller, delete or return the PI to the controller after the end of the provision of services by the processor;
- make available to the controller all information necessary to demonstrate compliance with the foregoing

obligations, and allow the controller to carry out an audit; and
- notify the controller immediately if any instruction received from the controller infringes the GDPR.

In June 2021, the European Commission published standard contractual clauses for use between controllers and processors, which are entirely optional.

Law stated - 24 May 2022

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The disclosure, knowingly or recklessly, of a person's PI by a processor, without the controller's prior authority is restricted under the Irish Data Protection Acts 1988 to 2018 and breaches of that restriction are subject to administrative or criminal sanctions, or both. In addition, a person who, without the prior authority of the controller or processor, obtains PI and discloses the PI to another person, commits a criminal offence. Similar offences also exist where a person sells, or offers to sell, PI that is obtained without the controller or processor's authority.

Law stated - 24 May 2022

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Pursuant to the GDPR, it is not permitted for PI to be transferred from within the European Economic Area (EEA) to a jurisdiction outside the EEA, unless a safeguarding mechanism is put in place, examples of which include the following.

- Adequacy decision: PI may be transferred to a jurisdiction in respect of which a finding of adequacy has been issued by the European Commission.
- Standard contractual clauses: PI may be transferred by a controller to another controller or processor pursuant to the European Commission's pre-approved standard contractual clauses. In In June 2021, the European Commission adopted updated standard contractual clauses (which have been drafted to reflect the requirements of the GDPR) to govern cross-border transfers of personal data outside the EEA and to replace the standard contractual clauses previously adopted by the European Commission. The updated standard contractual clauses entered into force on 27 June 2021, subject to an implementation period. Data transfer arrangements concluded before 27 September 2021 on the basis of the pre-existing standard contractual clauses shall be deemed to provide appropriate safeguards, within the meaning of the GDPR, until 27 December 2022 (provided the nature of the particular data transfer remains unchanged). The Court of Justice of the European Union (CJEU) in the Schrems II case upheld the continuing validity of standard contractual clauses. However, the CJEU also stated that controllers or processors, when acting as data exporters, should consider the particular data protection regime in the destination jurisdiction and put in place appropriate supplementary contractual measures to ensure that the transferred PI is protected. On 21 June 2021, the European Data Protection Board (EDPB) issued recommendations on measures that supplement data transfer mechanisms (the Recommendations). The Recommendations contain guidance on additional measures that may be implemented to ensure compliance with the requirements for data transfers, as set out in the GDPR. The EDPB's adoption of the Recommendations follows the CJEU's judgment in the Schrems II case.
- Binding corporate rules: PI may be transferred on the basis of intra-group binding corporate rules that have been

approved by the DPC or another data protection supervisory authority in another EEA jurisdiction.

Following the UK's departure from the EU, transfers of PI can continue to flow freely without putting in place any additional safeguarding mechanism pursuant to the adjudication of the European Commission as to the adequacy of the UK's data protection regime.

Law stated - 24 May 2022

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions that apply under the GDPR to transfers from within the EEA to outside the EEA, apply equally to transfers to service providers (processors) and to any onwards transfers.

The CJEU's findings in the Schrems II case provide a clear reminder that the protection granted to PI in the EEA must travel with the PI wherever it is transferred. The transfer of PI to third countries cannot result in the protection afforded to PI in the EEA being undermined. As such, PI that is transferred to another controller or processor outside the EEA pursuant to one of the safeguarding mechanisms provided for under the GDPR must be afforded the same protection when being further transferred by the initial recipient.

Law stated - 24 May 2022

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no data localisation requirements in Ireland under applicable laws, including the GDPR and the DPA.

Law stated - 24 May 2022

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the General Data Protection Regulation (GDPR), data subjects have the right to obtain from the controller (1) confirmation as to whether or not their PI is being processed by the controller and (2) where their PI is being processed. They also have the right to the following information:

- the purposes of the processing;
- the categories of PI being processed;
- the recipients or categories of recipients with whom the PI may, or has, been shared;
- the safeguards put in place in respect of any international transfers of the PI;
- the retention period for the PI;
- the existence of the rights available to them under the GDPR, including the right to make a complaint to the Data

Protection Commission (DPC) or other relevant data protection authority;
- where the PI was not collected from them directly, information as to the source of the data; and
- existence of any automated decision-making, details of and an explanation of the logic involved as well as the significance and the envisaged consequences of such processing for them.

In addition to the information listed above, controllers must provide data subjects with a copy of their PI, free of charge. Where the request is manifestly unfounded or excessive, the controller may charge a reasonable fee to cover administrative costs in complying with the request and may reject repeated identical requests.

Controllers must comply with the requirements set out above without undue delay and in any event within one month of receipt of the request (subject to extension in certain circumstances).

The Irish Data Protection Acts 1988 to 2018 (DPA) detail certain exceptions to a data subject's right of access. The restrictions on data subjects' access rights include where information is subject to legal privilege, where the information comprises an opinion of a third party given in confidence or where PI is processed for the purpose of estimating the amount of the liability of the controller on foot of a claim. In addition, the right of access to PI must not adversely affect the rights of third parties.

Law stated - 24 May 2022

Other rights

Do individuals have other substantive rights?

Individuals have the following additional substantive rights:

- the right to the rectification of their PI that is inaccurate;
- the right to the erasure or deletion of their PI in certain circumstances, for example, when the PI is no longer necessary for the purposes for which it was collected by the data controller;
- the right to object to the processing of their PI;
- the right to receive a copy of their PI in a structured, commonly used and machine-readable format, and to transmit that PI to another controller without hindrance, to the extent that it is technically feasible;
- the right to have the processing of their PI restricted in certain circumstances; and
- the right not to be subject to a decision based solely on the automated processing of PI, including profiling, except in particular circumstances.

Law stated - 24 May 2022

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under the DPA, a data subject may receive compensation for any material and non-material damage suffered as a result of their data privacy rights under the GDPR or the DPA, or both, having been infringed.

Law stated - 24 May 2022

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In circumstances where a data subject considers their data privacy rights under the GDPR or the DPA, or both, have been infringed, the data subject may bring a court action founded in tort against the controller or processor concerned. The Circuit Court, concurrently with the High Court, has jurisdiction to hear and determine such actions.

The DPC has no power to award compensation to affected individuals.

Law stated - 24 May 2022

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The General Data Protection Regulation (GDPR) provides that each EU member state may restrict the scope of certain obligations and rights created under the GDPR. Accordingly, the Irish Data Protection Acts 1988 to 2018 include a number of exceptions to the rules that apply generally to the processing of PI including the following:

- that the processing of PI for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with the GDPR;
- an exception from the requirement that PI be processed only in accordance with the purpose for which it was collected in the case of issues relating to national security or prosecution of criminal offences;
- an exception from controllers' obligations and limitation of data subjects' rights for important objectives in the public interest (eg, safeguarding national security); and
- a limitation on the exercise of data subjects' rights in relation to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Law stated - 24 May 2022

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The legal regime that currently applies to the use of cookies is the ePrivacy Directive 2002 and the Irish ePrivacy Regulations, which transpose the ePrivacy Directive 2002 into Irish law.

Additionally, where cookies contain identifiers that may be used to target a specific individual, or where information is derived from cookies and other tracking technologies that may be used to target or profile individuals, this will constitute PI and its processing is also subject to the General Data Protection Regulation (GDPR).

The Irish ePrivacy Regulations require website operators to obtain a website user's freely given, specific, informed and unambiguous consent to the setting of cookies on their device. The Data Protection Commission (DPC) noted in guidance issued in April 2020 that this is the same standard of consent as required by the GDPR and that consent is

required for the setting of cookies whether the cookies contain PI or not.

Law stated - 24 May 2022

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Organisations that wish to market by email, fax, telephone or other electronic channels must comply with the provisions of the GDPR, the Irish Data Protection Acts 1988 to 2018 and the Irish ePrivacy Regulations.

Pursuant to the Irish ePrivacy Regulations, an individual must give his or her freely given, specific, informed and unambiguous consent (eg, by specifically opting in) to receive any electronic marketing communications. The individual being targeted by the marketing communication may withdraw his or her consent to the communications at any time and has the right under the GDPR to object to the communications. In accordance with the principles of GDPR, the organisation issuing the marketing material must make the targeted individual aware of this right.

The Irish ePrivacy Regulations allow for direct marketing to take place without explicit consent in certain specific circumstances in the context of a sale of a product or service.

Under the Irish ePrivacy Regulations, marketing calls to mobile phones are prohibited unless:

- the caller has been notified by the targeted individual that he or she consents to the receipt of such calls on his or her mobile telephone; or
- the targeted individual has consented generally to receiving marketing calls to his or her mobile phone and such consent to receive marketing calls is recorded in the national phone directory.

Law stated - 24 May 2022

Targeted advertising

Are there any rules on targeted online advertising?

Targeted online advertising often involves a number of separate parties, including the providers of the platform via which the targeted advertisement is delivered (the platform) and the individuals or companies that seek to use the platform to target or direct certain advertisements or messages at data subjects. Each of these parties must ensure that the personal data that is processed in connection with the tailoring of the advertisements and delivery of those advertisements is processed in accordance with the provisions of the GDPR. This will include establishing a legal basis for the processing of the targeted individuals' personal data and processing that personal data in accordance with the data processing principles set out in the GDPR. Of particular relevance in the context of targeted advertising will be ensuring compliance with the 'transparency principle' under the GDPR, which requires those controllers to provide the data subjects that receive the targeted advertisement with complete details of the means by which the targeted advertisement has been delivered.

Compliance with the GDPR in this context will also require the providers of a platform and the targeting entities to consider whether they are in fact 'joint controllers' for the purposes of the GDPR and, if so, what legal basis they have for processing the relevant data subjects' personal data.

Finally, prior to commencing online targeting operations, controllers should examine whether the processing operations are 'likely to result in a high risk' and, accordingly, conduct a data protection impact assessment (DPIA). If the social media provider processes 'special categories of data' under the GDPR, which includes 'special categories of personal data', it must find a legal basis for the processing in article 6 GDPR and rely on an exemption, such as explicit consent.

The European Data Protection Board published guidelines on 2 September 2020 that provide further information on the legal considerations arising in the context of targeted advertising.

Law stated - 24 May 2022

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Under the GDPR 'special categories of personal data' include data about an individual's health, racial or ethnic origin, biometry, religious or philosophical belief, political opinion, trade union membership, sex life or sexual orientation. Article 9 of the GDPR prohibits the processing of these special categories of personal data, except in certain excepted circumstances.

Circumstances where the processing of special categories of personal data is permitted under the GDPR include where the data subject has given explicit consent to the processing of the personal data and where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security.

Based on the fact that the risks associated with processing special categories of personal data are higher, controllers and processors engaging in the processing of such personal data will be required to implement appropriate technical and organisational measures to ensure a level of security that is appropriate to that risk.

When processing special categories of personal data on a large scale, a controller is required to carry out a DPIA.

Law stated - 24 May 2022

Profiling

Are there any rules regarding individual profiling?

Article 22 of the GDPR states that a 'data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.

There are exceptions to this prohibition on decision-making based on automated processing, including where a particular decision is necessary for entering into, or performance of, a contract between the data subject and a controller, where expressly permitted under EU or EU member state law, or where the processing is carried out based on the data subject's explicit consent.

Where a controller utilises automated processing, the controller should employ suitable safeguards, which should include specific information of the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

Law stated - 24 May 2022

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The GDPR does not include any specific provisions relating to the use of cloud computing services or the outsourcing of activities by organisations to cloud service providers.

However, the DPC has issued guidance that details the security and transparency considerations that controllers

should consider when using cloud computing services or engaging cloud service providers. These considerations are based on the principles for data processing set out in the GDPR.

The guidance emphasises the importance of putting in place a GDPR-compliant contract between the controller and the cloud computing service (which will typically be a processor) and ensuring that a safeguarding mechanism is implemented for any transfers of PI to a cloud computing service or cloud service provider located outside the European Economic Area.

Finally, entities that are regulated by the Central Bank of Ireland or an equivalent regulatory authority may be subject to an extra layer of regulation in relation to the use of cloud computing services or outsourced service providers.

Law stated - 24 May 2022

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Various multinational big tech organisations are headquartered in Ireland and, as such, the Data Protection Commission (DPC) plays a significant global role in regulating their activities as competent supervisory authority. This means Ireland has been at the centre of a number of recent developments in international data protection, including changes to the regulation of international data transfers and significant enforcement proceedings under the General Data Protection Regulation (GDPR). In the past year, the DPC has issued a number of significant enforcement decisions and fines.

The year 2021 also saw the introduction by the European Commission of the new standard contractual clauses governing transfers of personal data to countries outside the EEA. The new standard contractual clauses were also accompanied by the issuance of the European Data Protection Board recommendations on measures that supplement transfer mechanisms following the Court of Justice of the European Union's Schrems II decision in 2020. The European Commission also adopted standard contractual clauses for use by controllers when appointing processors to process data on their behalf.

In the past year, the DPC has also been active in publishing detailed guidance in a number of areas including in relation to a child-oriented approach to data processing.

Law stated - 24 May 2022

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	Thompson Dorfman Sweatman LLP
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Legal Consultants
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
Mexico	OLIVARES
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitão, Galvão Teles, Soares da Silva & Associados

Singapore	Drew & Napier LLC
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP