



Glossary

The following terms used throughout this guide have specific legal meanings under the GDPR. In order to understand your rights fully, please read the following glossary of key terms.

GDPR

The General Data Protection Regulation (2016/679) is the new EU Regulation on Data Protection, which will come into force on the 25th May 2018.

Personal data

The term “personal data” means any information relating to a living person who is identified or identifiable (such a person is referred to as a “data subject”).

A person is identifiable if they can be identified directly or indirectly using an “identifier”. The GDPR gives examples of identifiers, including names, identification numbers, and location data. A person may also be identifiable by reference to factors which are specific to their identity, such as physical, genetic or cultural factors.

Processing

The term “processing” refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

Data Protection Commission

The “Data Protection Commission” (‘Commission’) is the body which will be established under Data Protection Act 2018 and which will replace the Data Protection Commissioner’s office. The Commission will be a supervisory authority i.e. an independent public authority, established under the GDPR, with responsibility for monitoring the application of the GDPR.

Data Controller

A “data controller” refers to a person, company, or other body which determines the purposes and means of processing of personal data.



Data Processor

A “data processor” refers to a person, company, or other body which processes personal data on behalf of a data controller.

Data subject

A Data subject is the individual the personal data relates to.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the GDPR. (More guidance about conducting DPIAs can be found on www.GDPRandYou.ie)

Data Protection by Design

Data Protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Protection by Default

Data Protection by default means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

Lawful basis for processing personal data

In order to process personal data you must have a lawful basis to do so. The lawful grounds for processing personal data are set out in Article 6 of the GDPR. These are: the consent of the individual; performance of a contract; compliance with a legal obligation; necessary to protect the vital interests of a person; necessary for the performance of a task carried out in the public interest; or in the legitimate interests of company/organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject).



Retention Policy

How long will your organisation hold an individual's personal data? This will be influenced by a number of factors. There may be legal requirements on your organisation, depending on your business type (e.g. medical council rules). Keep the data for the least amount of time that you can in accordance with the requirements of your business, store it securely while it is in your possession and make sure to delete it fully and safely at the appointed time.

Special Categories (sensitive) of personal data

This is defined in Article 9(1) of the GDPR as data 'which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

Consent

Some types of processing are carried out on the basis that you have given your consent. Under the GDPR, consent to processing must be freely given, specific, and informed. You cannot be forced to give your consent, you must be told what purpose(s) your data will be used for and you should show your consent through a 'statement or as a clear affirmative action' (e.g. ticking a box).

Consent is not the only lawful basis on which your personal data can be processed. Article 6 of the GDPR sets out a complete list of lawful purposes for processing personal data (please see footnote on page 5 of this guide).

Profiling

Profiling is any kind of automated processing of personal data that involves analysing or predicting your behavior, habits or interests.