Engaging Content
Engaging People

General Data Protection Regulation: Individual Perspective

Yvette Graham, ygraham@tcd.ie

Thanks to: Dave Lewis, Harsh Pandit, Kaniz Fatema, Irish Data Protection Commission

@ethicscanvas
ethicscanvas.org
hello@ethicscanvas.org

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SFI

The ADAPT Centre is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

Objectives this Week

- The aims of the General Data Protection Regulation (GDPR)
- GDPR Principles
- Individual Perspective: Your rights under GDPR
- Organisational Perspective and Issues
- Privacy Canvas Exercise
- Ethical vs Privacy concerns

The Fundamental Right of Data Protection

Data protection is a fundamental right set out in Article 8 of the **EU Charter of Fundamental Rights**, which states:

- Everyone has the right to the protection of personal data concerning him or her.
- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- Compliance with these rules shall be subject to control by an independent authority.

General Data Protection Regulation

- The General Data Protection Regulation (GDPR) came into force in 25 May 2018.
- General application to the processing of personal data in the EU
- Sets out extensive obligations on data controllers and processors, and provides strengthened protections for data subjects.
- GDPR is directly applicable as a law in all EU Member States
- Certain issues have further effect in national law.
  - In Ireland, this is the Data Protection Act 2018.

Key Roles in GDPR

- Data Subject: any person **whose personal data** is being collected, held or processed.
- Data Controller: A person, company, or other body which **decides** the purposes and methods of processing personal data.
- Data Processor: A person, company, or other body which processes personal data **on behalf** of a data controller.
- Controllers and Processors are **accountable** for processing of personal data to Supervisory Authority

Key Roles in GDPR: Supervisory Authority

- Supervisory Authority: Independent public authorities responsible for monitoring the application of GDPR in a member state
- In Ireland the Supervisory Authority is the Data Protection Commission
- The Commission is responsible for **monitoring** the application of the GDPR in order to **protect the rights and freedoms** of individuals in relation to processing.
- Commission role includes: promoting public awareness of risks/rules/safeguards/rights; handling data subject complaints; and cooperating with other data protection authorities in other EU member states.
- Violators of GDPR may be fined up to €20 million, or up to **4% of the annual worldwide turnover** of the preceding financial year, whichever is greater

What is Personal Data?

The term ‘personal data’ means any information concerning or relating to a **living person who is either identified or identifiable** (i.e. the ‘data subject’).

An individual could be identified, **directly or indirectly**, in particular by reference to an identifier such as a

- name, an identification number, location data, an online identifier (such as an IP address) or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Special categories of personal data

Certain types of sensitive personal data are subject to additional protection under the GDPR. The special categories are:

- Personal data revealing racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning a natural person's sex life or sexual orientation.

What is Data 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.
- Processing can involve automated or manual operations.

Principles for Personal Data Processing

Personal data shall be:

- Processed **lawfully, fairly and in a transparent** manner;
- Collected for specified, explicit and legitimate **purpose**s and not further processed in a manner that is incompatible with those purposes; (‘purpose limitation’);
- **Adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- **Accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (‘accuracy’);
- Kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed; (‘storage limitation’);
- Processed in a manner that ensures appropriate **security** of the personal data, (‘integrity and confidentiality’).

Lawful Basis for Personal Data Processing

Article 6 of the GDPR sets out the complete list of lawful reasons for processing personal data as:

1. **Consent**.
2. To carry out a **contract**.
3. In order for an organisation to meet a **legal obligation**.
4. Where processing the personal data is necessary to protect the **vital interests of a person**.
5. Where processing the personal data is necessary for the performance of a task carried out in the **public interest**.
6. In the **legitimate interests** of a company/organisation (except where those interests contradict or harm the interests or rights and freedoms of the individual)

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
- You should show your consent through a ‘statement or as a clear affirmative action’ (e.g. ticking a box).

Rights under GDPR

Right of:

- Access
- To be Informed
- Rectification
- Erasure (‘to be forgotten’)
- Portability
- On automated decision making
- To object to processing

Right of Access

You have the right to obtain the following:

- **Confirmation** of whether or not personal data concerning you is being processed.
- Where personal data concerning you is being processed, **a copy** of your personal data.
- Where personal data concerning you is being processed, other **additional information** as follows:
    - Purpose(s) of the processing.
    - Categories of personal data.
    - Any recipient(s) of the personal data to whom the personal data has or will be disclosed, in particular recipients in third countries or international organisations and information about appropriate safeguards.
    - The retention period or, if that is not possible, the criteria used to determine the retention period
    - The existence of rights to: rectification; erasure; restrict processing; object; and how to request these from the controller.
    - The right to raise a concern with a supervisory authority (in Ireland this is the Data Protection Commission).
    - Where personal data is not collected from the data subject, any available information as to its source.
    - The existence of automated decision-making, including profiling and meaningful information about how decisions are made, the significance and the consequences of processing.

Right to be Informed

- It should be **clear and transparent** to individuals that personal data concerning them are collected, used, consulted or otherwise processed, and to what extent the personal data are, or will be, processed.
- The principle of transparency: any information on the processing of personal data must be
  - Easily accessible
  - Easy to understand,
  - In clear and plain language – including visualisations
- Individuals should be **made aware of** risks, rules, safeguards and rights in relation to the processing of personal data.
- In particular, the **specific purposes** for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.

Right to Rectification

If your personal data is inaccurate, you have the right to have the **data rectified**, by the controller, without undue delay.

If your personal data is incomplete, you have the right to have **data completed**, including by means of providing supplementary information.

The right of rectification is **restricted** for important objectives of public interest, and for balance with the right of freedom of expression and information.

Right to Erasure (a.k.a. Right to be Forgotten)

You have the right to have your data erased by the data controller, if one of the following grounds applies:

- Where your personal data are **no longer necessary in relation to the purpose** for which it was collected or processed.
- Where you **withdraw your consent** to the processing and there is no other lawful basis for processing the data.
- Where you **object to the processing and there is no overriding legitimate grounds** for continuing the processing or your personal data are being processed for direct marketing purposes.
- Where your personal data have been **unlawfully processed**.
- Where your personal data have to be erased in order to comply with **a legal obligation**.
- Where your personal data have been collected in relation to the offer of information society services (e.g. social media) to a child.

The data controller must **communicate any rectification or erasure to each recipient** to whom the personal data have been disclosed, and inform you about recipients if requested

Exception where processing is necessary for:

- Exercising the right of freedom of expression and information.
- Compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority.
- Reasons: of public interest in the area of **public healt**h, of **archivi**ng in the public interest, of **scientific or historical research** purposes or **statistical purposes**.
- Establishment, exercise or defence **of legal claims**.

Right to Portability

In some circumstances, you may be entitled to obtain your personal data from a data controller in a **format that makes it easier to reuse** your information in another context, and to transmit this data to another data controller of your choosing without hindrance.

This right only applies where processing of personal data is carried out by automated means, and where you have either consented to processing, or where processing is conducted on the basis of a contract between you and the data controller.

This right only applies to the extent that it **does not affect the rights and freedoms of others.**

Where this right applies, data controllers must provide and transmit personal data in **structured, commonly used and machine-readable form**.

Rights on Automated Decision Making

You have the right to **not be subject** to a decision based **solely on automated processing**. Processing is "automated" where it is carried out without human intervention and where it produces legal effects or significantly affects you.

Automated processing includes profiling. Profiling is any kind of automated processing of personal data that involves **analysing or predicting your behaviour, habits or interests.**

Automated processing is permitted only

- with your express consent,
- when necessary for the performance of a contract or
- when authorised by Union or Member State law.

Where one of these exceptions applies, suitable measures must be in place to safeguard your rights, freedoms and legitimate interests. This may include

- the right to **obtain human intervention** on the controller's part,
- the right to **present your point of view**, and
- the right to **challenge the decision**.

Right to Object to Processing

You have the right to object to certain types of processing of your personal data where this processing is carried out in connection with tasks:

- in the public interest,
- under official authority, or
- in the legitimate interests of others.

You have a stronger right to object to processing of your personal data at any time where the processing relates to **direct marketing**.

You may also object to processing of your personal data for **research purposes**, unless the processing is necessary for the performance of a task carried out in the public interest.

Where the right to object applies, data controllers are obliged to notify you of this at the time of their first communication with you. Where processing is carried out online, data controllers must offer an online method to object.

Right to Restriction

You have a **limited right of restriction** of processing of your personal data by a data controller.

Where processing of your data is restricted, it can be stored by the data controller, but most other processing actions, such as deletion, will require your permission.

This right applies in four ways.

- where you have **objected to processing** of your data
- where you have **contested the accuracy** of your data
- where processing is **unlawful**.
- where you require data for the **purpose of a legal claim**.

Where you have obtained restriction of processing of your data, the data controller must inform you before lifting the restriction.

Limitations on Individual Rights

- The right to data protection is **not an absolute right**.
- It must always be balanced against other values, fundamental rights, human rights, or public and private interests.
  - For example, your right to access your data should not adversely affect the rights and freedoms of **others**.
- In limited circumstances, organisations, may **charge a reasonable fee** for responding to a request, or even to refuse to respond if it is manifestly unfounded or excessive.
- Organisation must always respond to your requests within **one month,** even if they plan to refuse it.
- If refusing a request, an organisation must set out clearly which limitation or restriction they are relying, their reasons for for doing so, and the possibility of lodging a complaint.

Complaining to Supervisory Authority

There are three types of access request complaints:

- **No response** to an access request.
- **Incomplete** response to an access request.
- Exemptions to withhold data being **applied incorrectly**.

For example, if you believe a data controller has not responded in full to your access request, provide the DPC:

- A copy of the access request.
- Signed authority from you where a solicitor/representative has made the contact.
- A copy of any letter sent to the data controller outlining the specific personal data that has not been provided.
- Any evidence you have of the existence of the personal data concerned.
- Any other relevant correspondence on the matter.
- Exemptions being used to withhold data that may be applied incorrectly