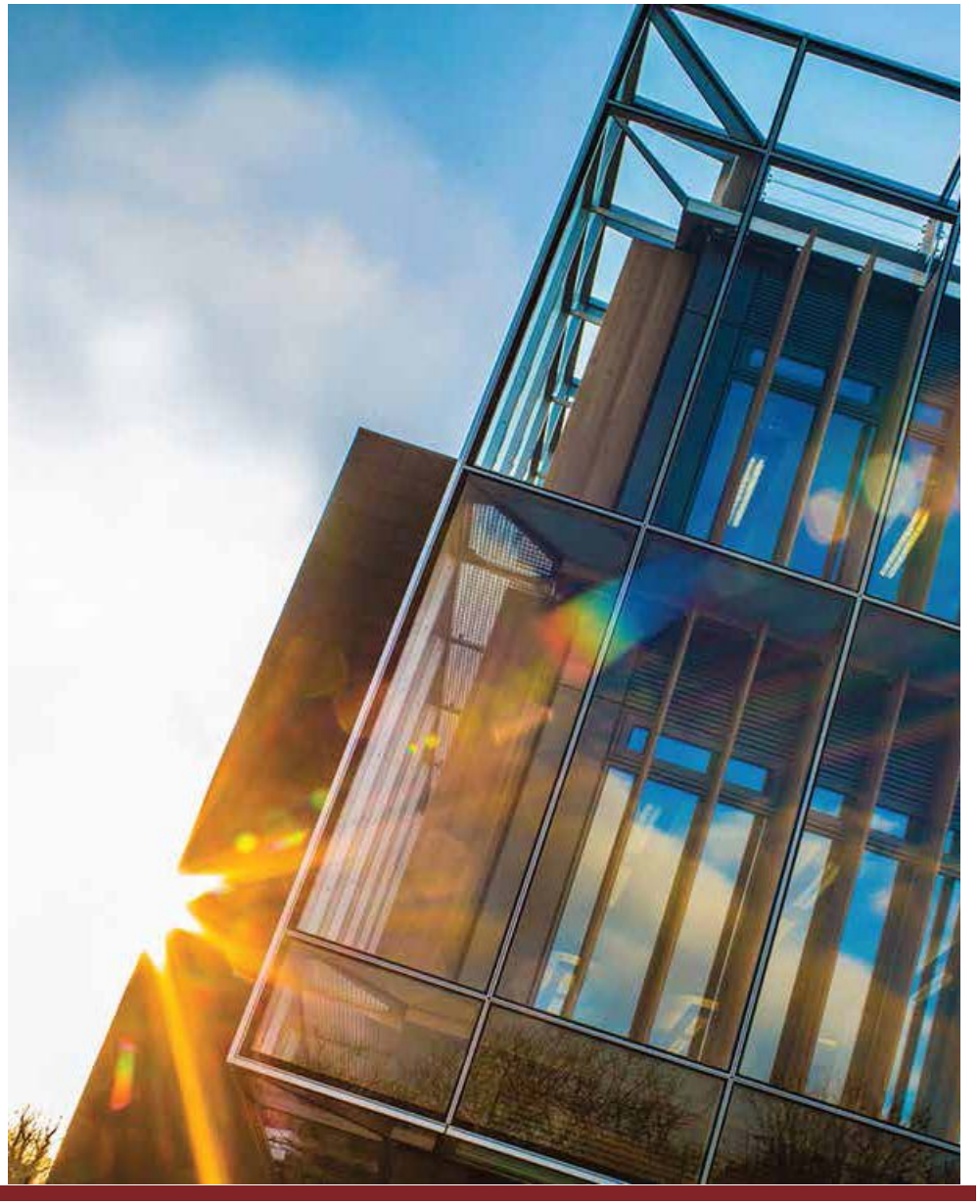
Maynooth University
National University of Ireland Maynooth



GENERAL DATA PROTECTION REGULATIONS (GDPR)

A Changing Data Protection Landscape and what it means for MU

Changing Data Protection Legislation

- **1988 – Irish Data Protection Act**

  Office of the Data Protection Commissioner established.

- **1995 – EU Directive**

  Established a common framework across the EU.

- **2003 – Irish Data Protection Act**

  Updated Irish legislation to implement EU Directive.

- **2017 – EU General Data Protection Regulation (GDPR)**

  Harmonised disparate EU laws. Directly effective.

- **2018 – May 25th – GDPR came into force. Data Protection Act 2018 signed into Law.**

What is Data Protection?

- Data Protection is about an individual's fundamental right to **privacy**.
- When an individual gives their personal data to an organisation, the recipient has a duty to keep these details private & safe.
- Governs the way in which we deal with personal information (data).
- Mechanism for safeguarding privacy rights of individuals in relation to the processing of their personal data.
- Upholds rights/enforces obligations.
- Overseen by Office of the Data Protection Commissioner (DPC) who has significantly increased powers.

Definition: Personal Data

Data relating to *living, identifiable* individuals.

Current Definition

"Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is, or is likely to come into, the possession of the data controller."

GDPR Definition

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

Applies to manual ***and*** electronic data.

Definition: Special Categories of Personal Data (Sensitive Personal Data)

- Racial origin;
- Political opinions;
- Religious or philosophical beliefs;
- Racial origin;
- Trade Union membership;
- Genetic Data (e.g. biological samples);
- Biometric Data (e.g. fingerprints, facial recognition);
- Data concerning health;
- Data concerning a person's sex life or sexual orientation;
- **Explicit consent required to process special categories of personal data**.

Definition: Processing

Performing any operation on personal data, whether or not by automate means, including:

- Obtaining;
- Storing;
- Transmitting;
- Recording;
- Organising;
- Altering;
- Disclosing;
- Erasing.

GDPR applies to:

- **Data Subjects** (e.g. staff, students, research subjects, members of the public);
- **Data Controllers** (e.g. MU, some research centres/projects);
- **Data Processors** (those who process data on behalf of data controllers).

GDPR applies where one of the above is based in the EU (e.g. GDPR applies to organisations based ***outside*** the EU if they collect or process personal data of EU citizens).

Why is GDPR important?

- People increasingly aware of their rights – expect organisations to protect their personal data;
- Investigations/audits by the Office of Data Protection Commissioner;
- Can be forced to release information or can be taken to the Courts by the Data Subject directly;
- Data security breaches;
- Negative publicity and loss of “consumer” confidence.

What is GDPR?

The principles (rules) of GDPR are similar to current DP Acts, with added detail and new Accountability principle:

- Lawfulness (consent, legitimate interest…);
- Fairness and Transparency;
- Purpose Limitation;
- Accuracy;
- Data Minimisation;
- Retention;
- Security;
- Accountability;
- Rights of Data Subjects.

What is GDPR (Contd):

Key changes to Principles:

- More information must be given to data subjects (how long data will be kept, right to lodge a complaint to ODPC, source of the data…);
- Must explain and document legal basis for processing personal data;
- GDPR tightens the rules on how consent is obtained (must be freely distinguishable from other matters and in clear plain language);
- Must be as easy to withdraw consent as it is to give it;
- More flexibility on “legitimate interests” as a lawful ground to process personal data in some circumstances, but must inform people if you are relying on this.

What is GDPR (Contd)?

- Single set of Rules and “One Stop Shop” (one supervisory authority for organisations who are based in multiple countries);
- Privacy Impact Assessments (mandatory in certain circumstances);
- Privacy by Design & Default;
- Subject Access, rectification right to object to certain processing e.g. marketing
- New rules on profiling (explicit consent required).

What is GDPR (Contd)?

- **Mandatory notifications of Data Security Breaches**
  - to Data Protection Commissioner within 72 hours;
  - to Data Subjects “without undue delay”.

- **The law will apply to Data Processors as well as Data Controllers** (extensive new requirements to be imposed on contracts);

- **Transposition into Irish Law** – Data Protection Act 2018 signed into Law on May 25th

- Clarity on issues.

GDPR Preparations in MU

- Steering Committee;
- Project Plan;
- Data mapping process;
- Review/update of consent forms and privacy notices;
- Online training module on GDPR for all staff and research students
- Data Protection webpage updated;
- University News and Staff News and other means used to re-enforce the message that GDPR is everyone's business.

GDPR – Risks at MU

- Not being aware of personal data held by MU;
- Data held locally;
- Sensitive personal data
- Retention schedules not adhered to (IA already identified issues with research data but not sure if it is personal data)
- Breach notification;

Appendices: Principles of GDPR (The Rules)

1. Lawfulness
2. Fairness and Transparency
3. Purpose Limitation
4. Accuracy
5. Data Minimisation
6. Retention
7. Security
8. Accountability
9. Rights of Data Subjects
10. Personal Data Security Breaches

Appendix 1: Lawfulness

Processing shall be lawful only if and to the extent that at least one of the following applies:

- Consent;
- Necessary for the performance of a contract;
- Necessary for compliance with a legal obligation;
- Necessary to protect the vital interests of the data subject or another person;
- Necessary for the performance of a task carried out in the public interest;
- Necessary for the purpose of the legitimate interests.

Appendix 2: Fairness and Transparency

At the time personal data is being collected from data subjects, they must be informed via a "**Data Protection Notice"** of the following:

- The identity and contact details of the data controller;
- The contact details of the data protection officer;
- The purpose of the processing and the legal basis for the processing;
- The recipients or categories of recipients of the data;
- Details of any transfers out of the EEA, safeguards in place and the means by which to obtain a copy of them;
- The data retention period used or criteria to determine same;
- The individual's rights (access, rectification and erasure, restriction, objection, complaint,).

Appendix 3: Purpose Limitation

Personal data must be processed for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes.

- Be clear about why you are collecting personal data;
- Make sure that data subjects are also clear about the purpose(s) for which you are collecting/holding their data and what they might be contacted about;
- Cannot expand purpose without reverting to individual.

Appendix 4: Accuracy

Personal data shall be 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.

- The longer personal data is held, the more likely it will be inaccurate and out-of-date;
- Individuals have the right to have errors rectified;
- Staff must ensure that local procedures are in place to ensure high levels of personal data accuracy, including periodic review and audit.

Appendix 5: Data Minimisation

Personal data must be adequate and relevant.

Limited to what is necessary in relation to the purpose for which it is processed.

- Must seek and retain only the **minimum** amount of personal data from data subjects which you need to achieve your purpose;
- Advisable to carry out periodic reviews of data being sought and data already held.

Appendix 6: Retention

Controllers and processors are required to maintain records of processing activities and to make them available to the DPC on request.

- You must be clear about length of time data will be kept and reason for same. Data should never be kept "just in case";
- Decide how long data should be kept for;
- Records Management Policy/ Retention Schedules;
- SOP re Disposal of redundant personal data.

Appendix 7: Security

Personal data must be processed in a manner that ensures appropriate security of the personal data, incl. protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- "Appropriate security measures" (appropriate to the harm that might result and to the nature of the data);
- *May have regard to cost of implementation;*
- *May have regard to the current state of technology;*
- *Staff must know and comply with measures;*
- *Internal review of security measures - part of Internal Audit function;*
- Extremely important to make sure that all personal data you are responsible for is kept secure and in such a way that it does not permit unauthorised access, intentionally or accidentally.

Appendix 8: Accountability

The GDPR introduces a new concept of accountability, which requires controllers to maintain records of processing activities in order to demonstrate how they comply with the data protection principles.

- Inventory of personal data;
- Providing assurance about DP compliance;
- Data Privacy Impact Assessments;
- Need to document:
  - Why it is held;
  - How it is collected;
  - When it will be deleted;
  - Who may gain access to it.

Appendix 9: Rights of Data Subjects

- Right of Access (copy to be provided within one month);
- Right to Erasure;
- Right to Restriction of Processing;
- Right to object to Processing;
- Right not to be subject to a decision based solely on automated processing.

Appendix 10: Personal Data Security Breaches

What is a Personal Data Security Breach?

- Disclosure of confidential data to unauthorised individuals;
- Loss or theft of data or equipment on which data is stored;
- Hacking, viruses or other security attacks on IT equipment/ systems/networks;
- Inappropriate access controls allowing unauthorised use of information;
- Emails containing personal data sent in error to wrong recipient;
- Applies to paper and electronic records;
- Consequences: Financial, Reputational, Legal...

Appendix 10: Personal Data Security Breaches (Contd)

- Breaches managed by **Data Protection Officer.**

- **What to do if you discover a breach (or potential breach)?**
  - Don't delay – act immediately;
  - Report incident;
  - This enables University to assess, contain and respond to incident (incl. notifying affected parties and DPC).

- **Law requires mandatory breach notifications:**
  - **to DPC within 72 hours**
  - **to data subjects "without undue delay".**

Contact

Ann McKeon

Data Protection/Freedom of Information Officer

Humanity House

South Campus

Tel: 01 7086184

Email: ann.mckeon@mu.ie

Web: https://www.maynoothuniversity.ie/data-protection