Policy Title:	Guidelines on GDPR for Research Purposes
Description:	The purpose of a General Data Protection Regulation (GDPR) is to impose a uniform level of data protection and security for organisations, researchers and other actors. Due to the global importance in trade and international science, GDPR will have an impact on personal data protection requirements in research.
Author (Position):	Vice President (Academic Affairs) and Registrar
Version:	2
Approved By:	MIE Governing Body
Policy Approval Date:	January 2019
Date of Next Policy Review:	April 2023 (or as necessary)

Guidelines on GDPR for Research Purposes

1 Context

1.1 The European Union (EU) General Data Protection Regulation (GDPR), 2018 regulates the processing of personal data relating to individuals when:

1.1.1 Personal data is processed by a data controller or processor situated within a European Economic Area (EEA) Member State in an EU Member State; or

1.1.2 The processing relates to individuals, irrespective of nationality, situated within the EEA (even if the controller/processor is situated outside of the EEA).

1.2 The purpose of GDPR is to impose a uniform level of data protection when data is being processed within, or being transferred to other Member States within the EEA. This puts organisations, researchers and other actors on a level playing field when it comes to personal data security and protection. Due to the global importance in trade and international science, GDPR will have an impact on personal data protection requirements.

1.3 The privacy and data protection requirements of GDPR include:

1.3.1 Informed, unambiguous and clear consent of data subjects to data processing.

1.3.2 The need for heightened security measures and organisational practices to be implemented, depending on the type of personal data that is processed and the nature of the processing.

1.3.3 The need to anonymise or pseudonymise personal data as soon as possible to protect the data subject's privacy.

1.3.4 The provision of personal data breach notifications to authorities (in this case the Data Protection Commission of Ireland).

1.3.5 Requirements for the secure transfer of personal data across borders

1.3.6 The need for certain organisations to mandatorily appoint a Data Protection Officer (DPO) to oversee compliance with data protection law.

2 Definitions

2.1 **Data Controller** – The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.2 **Data Processor** – The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2.3 **Consent** – Consent is defined as receiving a data subject's agreement to process their data. It must be freely given, informed, specific and unambiguous.

2.4 **Data Breach** – Unlawful destruction, loss, alteration, unauthorised disclosure or access of a data subject's data.

2.5 **DPO** – An appointed individual who works to ensure implementation and compliances with policies and procedures set by GDPR.

2.6 **Data Subject** – Someone 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

2.7 **Data Protection Impact Assessment** – A tool used to identify privacy risks.

2.8 **Processing** – Any activity relating to personal data, from initial collection through to final destruction. This includes: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.9 **Pseudonymisation** – Processing data so it can no longer be attributed to data.

3 What is Personal Data?

Personal data is any information which can be directly or indirectly linked to an identifiable, living person. This definition means that a wide range of data is personal including (but not limited to): IP addresses, names, identification numbers, location data, online identifiers, photos, recordings (voice or visual), CCTV, car registration numbers, etc.

Sensitive person data is also defined, and afforded additional protection, under GDPR. This is categorised as 'Special Category Data' and relates to the processing of personal data revealing 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.

3.1 **Personal Data in Research**

The processing of personal data in research projects must comply with GDPR. Apart from the need to comply with the Regulation, additional requirements are imposed by funders, journals and the institutions to which international collaborators belong. It is also important to remember that accountability and ethics are fundamental to the Regulation and must be taken into account when processing to ensure that the data subject's rights are protected.

There are potentially grave economic consequences for non-compliance with GDPR, including fines of up to 4% of global turn over or €20 million (whichever amount is higher). There are also personal responsibility fines that can be imposed at executive level within an organisation if purposeful negligence, wilful ignorance or non-compliance can be proven.

4 What Must a Researcher do to Comply with GDPR?

4.1 Before the project -

4.1.1 All projects involving the collection, handling and or processing of personal data must be registered with the Institute.

4.1.2 If personal data is entrusted to external processors who are to perform a task or handle the data for the Institute, a GDPR compliant data processing agreement, which includes specific provisions, must be concluded and signed by the Head of Department. A copy must be sent to the Registrar's Office to Registrar@mie.ie and to dataprotection@mie.ie.

4.1.3 For data processors situated outside of the EEA, Standard Contractual Clauses must be used, as the agreement with data processors may be adapted depending on the nature of the controller & processors arrangement. This must then be signed by the Head of the Department. A copy must be sent to the Registrar's Office.

4.1.4 Project managers who grant students access to research data must enter into a data processing agreement with the individual student, examples of which can be requested from the GDPR administrator at dataprotection@mie.ie or can be found in the internal shared drive called "28GDPR", within the "Data Processing Agreements" folder.

4.1.5 Create a project – identification (ID) list. The ID list must be the only document/key connecting the data subject's personal data with his or her name or other identifiers.

4.1.6 All study documents and samples must be identified only by project – ID (pseudonymised).

4.1.7 The ID list must be stored in a folder on the project manager's hard drive or on the shared drive if required to share this with colleagues.

4.1.8 Implement a "Good Data Management Procedure" for the handling of personal data & train staff in these procedures[1].

4.1.9 Each project manager is responsible for carrying out a Data Protection Impact Assessment pursuant to Article 35 GDPR if personal data is used or being processed in research. If the processing may result in a high risk to the participants, the GDPR administrator/President's Office/Registrar's Office should be informed.

4.2 It is important to note – each individual utilising personal data is responsible for that data and the onus lies with them to ensure compliance with the regulation and any other laws that may apply.

4.3 For research that is especially at risk of identifying participants, or may involve sensitive personal data, as detailed on Page 2, permission from the Marino Ethics Research Committee (MERC) is required.

4.4 It is of the utmost importance that data subjects are completely informed of any implications to their participation and that they are made aware of their enhanced rights under GDPR to rescind this consent at any time during, or after the process.

4.5 All researches must be able to demonstrate evidence of consent if processing personal data and must archive informed consent forms or other documentation within locked cabinets or on password protected desktops or laptops.

4.6 New data processing agreements must be completed if new processors become involved & ID lists are also to be updated as the information contained within the research gains new participants.

4.7 Where personal data is no longer required, it can be archived in relation to the project. However, it must not be stored without being anonymised.

4.8 If a data breach or unauthorised disclosure is discovered it is of the utmost importance to report this to the dataprotection@mie.ie email, to contact the data subject and

[1] Record Management Policy and MIE Records Retention Schedule

inform them of the breach as well as work with the Data Protection Administrator within the Institute to complete a breach notification form.

4.9 After the Project

A project can only be viewed when it has ended and if its contents are anonymised correctly, utilising an ID list.

4.9.1 Please find further guidance from the Data Protection Commission on anonymisation and pseudonymisation.

Further guidance exists on the Irish Data Protection Act, 2018 pertaining to research.

5 Research & 'Growing up in Ireland' data

Researchers within the Institute are permitted to utilise data from the Growing up in Ireland (GUI) National Longitudinal Study of Children, as long as they have followed the outlined steps and have taken reasonable steps to ensure the safety of the data, in accordance with the requirements stipulated. Though the GUI is carried out pursuant to the Statistics Act, 1993 rather than the GDPR, it is important to incorporate the spirit of data protection while working with this data and to remember to treat this data with care.

6 Related Documents

6.1 Ethics in Research Policy

6.2 Procedure for Ethical Approval of Research Proposals

6.3 Policy on Managing Research Grants and Contracts

6.4 Good Research Practice Policy

6.5 Lone Researcher Guidelines

6.6 MIE Privacy Statement

6.7 Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018

6.8 Record Management Policy

6.9 MIE Records Retention Schedule