

**Data Protection Impact Assessment (DPIA)**

**Author / Policy Owner:** Data Protection Office

**Creation Date:** 7th March 2018

**Review Date:** 29th November 2022

**Scope:** This process applies to all new Maynooth University projects which will involve processing of Personal Data

**Related Policies:** Student Data Privacy Notice

 Staff Data Privacy Notice

 Maynooth University Retention Schedules

 Personal Data Security Breach Management Procedures

**Contact Details** dataprotection@mu.ie

 Room 27, Rye Annex, North Campus, Maynooth University

**Project Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Project Leader:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Contact Details:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Submitted to the Data Protection Office on \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved by the Data Protection Office on \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Maynooth University

Data Protection Office

# Revision History

|  |  |
| --- | --- |
| Date of this revision: 29th November 2022 | Date of next review: 21st November 2024 |

# Table of Contents

Project Title / Contact Details 1

[Revision History 2](#_Toc512359748)

[Table of Contents 3](#_Toc512359749)

[1. Purpose 4](#_Toc512359750)

[2. Introduction 4](#_Toc512359751)

[3. Definitions 4](#_Toc512359757)

[4. Background, Use and Functionality of the Project 5](#_Toc512359764)

[5. Data Protection Risks and Mitigations 6](#_Toc512359776)

## Purpose

The purpose of this document is to: (i) consider the privacy risks and the potential impact upon the relevant individuals in respect of the Project; and (ii) to set out the mitigations that will be put in place to minimise those risks and to minimise any negative impact from a data protection compliance perspective.

## Introduction

* 1. Maynooth University (“**MU**”) has prepared this Data Protection Impact Assessment (“**DPIA**”) in respect of the processing of Personal Data, including Special Categories of Personal Data, as part of the proposed (insert project name) \_\_\_\_\_\_ (the “**Project**”) in accordance with the GDPR and the Data Protection Act 2018.
	2. The purpose of this DPIA is to identify any areas of “high risk” from a data protection perspective and to identify what mitigations can be put in place to minimise the risk and ensure that the use of personal data complies with applicable laws.

## Definitions

See: <https://www.dataprotection.ie/en/individuals/data-protection-basics/definition-key-terms>

* 1. **Controller** or **data controller** refers to a person, company, or other body which decides the purposes and methods of processing personal data.
	2. **Processor** or **data processor** refers to a person, company, or other body which processes personal data on behalf of a data controller.
	3. **Data Subject** refers to a living person who is either identified or identifiable and is the subject of personal data.
	4. **Personal Data** means any information concerning or relating to a living person. 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.
	5. **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.
	6. **Special Categories of Personal Data** certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are:
1. Personal data revealing racial or ethnic origin.
2. Political opinions
3. Religious or philosophical beliefs
4. Trade Union Membership
5. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person
6. Data concerning health.
7. Data concerning a natural person’s sex life or sexual orientation

Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR.

## Background, Use and Functionality of the Project

* 1. Background

It is intended to initiate the Project to study \_\_\_\_. The Principal Investigator is \_\_\_\_\_\_\_\_. The ethics protocol for the Project was first approved on \_\_\_, under protocol number \_\_\_.

Give a brief description of the project/study:

e.g. how the study will be done? Will informed consent be obtained (if applicable)? where were the samples/details processed and stored? Will the data be annonymised/pseudonymised?

* 1. What data will be processed?

Please list the Personal Data which will be processed, e.g. name, contact details etc.

* 1. Proposed Use of the Personal Data

Please explain how it is intended to use/process the Personal Data.

Please also include any further relevant details.

* 1. Data Flows

Please give a list of any third parties who will receive Personal Data and a description of how the data will be shared with them.

* 1. Proportionality and Necessity

Please set out an assessment of the necessity and proportionality of any proposed processing of Personal Data in the context of the purposes of the processing.

* 1. Data Transfers

Please confirm whether there are transfers of Personal Data to countries which have not been found by the EU Commission to provide an adequate level of data protection? If so, please confirm the basis of such transfer, e.g. Privacy Shield or a data processing agreement incorporating the model clauses in the form approved by the EU Commission.

## Data Protection Risks and Mitigations

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation***[Please provide details of the information provided to data subjects]* |
| MU fails to comply with its notification obligation under the GDPR.  |  |
| Sensitive personal data may be collected. |  |
| Personal Data may be disclosed to third parties. |  |
|  |  |

* 1. Personal data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation** |
| Personal Data may be used for a purpose for which affected individuals may be unaware. |  |
| MU may not obtain fully informed and freely given consent from the relevant data subjects (where this is the lawful basis for processing). |  |
|  |  |

* 1. Personal data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation***[Please detail security measures taken]* |
| The security of the Personal Data could be compromised, e.g. Personal Data could be used, accessed, altered or removed without authorisation. |  |
|  |  |

* 1. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation***[Please detail steps taken by MU to minimise the Personal Data processed]* |
| The same result could have been achieved without processing Personal Data or by processing less Personal Data. |  |
|  |  |

* 1. Personal data shall be accurate, and, where necessary, kept up to date

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation***[Please detail steps taken by MU to ensure that the Personal Data remains accurate]* |
| MU might process Personal Data that contains inaccuracies. |  |
|  |  |

* 1. Personal **data shall be kept for no longer than is necessary for the purposes for which the data are processed**

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation**[*Please insert relevant retention period and rationale behind that retention period*] |
| Personal Data may be retained for longer than is necessary for the purposes for which the Personal Data is collected and processed, e.g. indefinitely. |  |
|  |  |

* 1. **Data Subject Rights**

|  |  |
| --- | --- |
| **Key Risks**  | **Mitigation** |
| A Data Subject may not be adequately informed of their rights  | *[MU to provide details of the steps taken to ensure that Data Subjects are provided with such information, e.g. via the relevant data protection notice]* |
| If a Data Subject withdraws their consent or requests the erasure of their Personal Data, MU may not be in a position to comply, especially where such Personal Data has been disclosed to third parties.  | *[MU will have a written agreement in place with any processors to ensure that they can comply with any relevant Data Subject rights including the right to withdraw consent. MU will also ensure the flow-down of such obligations to any sub-processors.]* |
|  |  |

* 1. **Transfer of Data Outside of the EEA (if applicable)**

|  |  |
| --- | --- |
| **Key Risks**  | **Mitigation** |
| Personal Data may be transferred to a country which has not been found by the EU Commission to provide an adequate level of data protection, without putting the necessary protections in place.  | *[Please detail protections put in place to ensure that such transfers are made in compliance with the GDPR, e.g. putting standard contractual clauses in the form approved by the EU Commission in place.]* |
|  |  |

Maynooth University Data Protection Office

**T** +353 1 708 3654 **E** dataprotection@mu.ie **W** maynoothuniversity.ie