

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

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

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

**Data Privacy Impact Assessment**

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

**Creation Date:** 7th March 2018

**Review Date:** 6th March 2019

**Version:** 20th August 2018

**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

Personal Data Security Breach Management Procedures

Maynooth University

Data Protection Office

# Revision History

|  |  |
| --- | --- |
| Date of this revision: | Date of next review: 6th March 2019 |

# Table of Contents

[Revision History 2](#_Toc512359748)

[Table of Contents 3](#_Toc512359749)

[1. Purpose 4](#_Toc512359750)

[2. Introduction and Methodology 4](#_Toc512359751)

[3. Definitions 4](#_Toc512359757)

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

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

[6. Consultation 8](#_Toc512359797)

[7. Contact 9](#_Toc512359798)

## 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 and Methodology

* 1. Maynooth University (“**MU**”) has prepared this Privacy Impact Assessment (“**PIA**”) 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 Acts 1988 to 2018. In order to prepare this PIA, the relevant experts including [*insert* *individuals, e.g. DPO*] as well as [*insert other methods taken to gather information in respect of this PIA including consultation with stakeholders*]. This helped to identify privacy risks prior to preparing the PIA.
  2. PIA’s are important as they allow us to anticipate and address the likely privacy impact of projects, processes, systems and technologies, in order to identify privacy related issues, develop solutions, and ensure that such issues are addressed appropriately in a manner consistent with statutory obligations and company policies.
  3. The purpose of this PIA 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.
  4. MU as the controller in respect of any Personal Data processed as part of the Project places a high priority on the protection of the privacy of such third parties. It demonstrates its commitment to “privacy by design” and “privacy by default” through the implementation of appropriate technical and organizational measures are designed to implement the data protection principles and ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility.
  5. Statutory obligations under the GDPR and the Data Protection Acts 1988 to 2018 place obligations on MU in respect of personal data for which it is the controller. For further information on how MU complies with such obligations, please see the Data Protection Policy.

## Definitions

* 1. **Controller** or **data controller** means any person who, either alone or with others, controls the purposes and means of the processing of personal data. Controllers can be either legal entities such as universities, companies, government departments or voluntary organisations, or they can be individuals.
  2. **Processor** or **data processor** means a person who processes personal data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his/her employment.
  3. **Data Subject** means an individual who is the subject of personal data.
  4. **Personal Data** means information relating to a living individual who is or can be identified either directly or indirectly, including by reference to an identifier (such as a name, an identification number, location data or an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual). This can be a very wide definition depending on the circumstances.
  5. **Processing** means performing any operation or set of operations on personal data including: (a) recording the personal data; (b) collecting, organising, structuring, storing, altering or adopting the personal data; (c) retrieving, consulting or using the information or personal data; (d) disclosing the personal data by transmitting, disseminating or otherwise making it available; or (e) aligning, combining, restricting, erasing or destroying the personal data.
  6. **Special Categories of Personal Data** means personal data relating to an individual’s: racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; physical or mental health, including in relation to the provision of healthcare services; sex life or sexual orientation. Individuals have additional rights in relation to the processing of any such data.

## Background, Use and Functionality of the Project

* 1. Background**[[1]](#footnote-1)**

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 \_\_\_.] (Insert a few sentences on the background – 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 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

* 1. This section details the main data protection responsibilities relating to the Project, the key risks and how the Project mitigates such risks. All such risks are risks to data subjects, but may also, due to risks of non-compliance with relevant legislation, be risks to MU (as controller).

We have identified the following considerations as relevant to the question of whether a PIA would be appropriate in relation to the processing of personal data as part of the Project:

* + 1. [The Project involves the collection and processing of Personal Data which might not otherwise take place;
    2. New Personal Data will be generated, including [insert description of personal data];
    3. Personal Data will be disclosed to organisations and/or individuals who would not previously have had routine access to it; and
    4. Personal Data will transfer outside of the EU.

Having regard to these factors MU was of the view that it would be beneficial in the circumstances to carry out a PIA in relation to the processing of Personal Data as part of the Project.

* 1. **Personal data must be obtained and processed fairly, lawfully and in a transparent manner**

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation** |
| MU fails to comply with its notification obligation under the GDPR. | *[Please provide details of the information provided to data subjects]* |
| 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** |
| The security of the Personal Data could be compromised, e.g. Personal Data could be used, accessed, altered or removed without authorisation. | *[Please detail security measures taken]* |
|  |  |

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

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

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

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

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

|  |  |
| --- | --- |
| **Key Risks** | **Mitigation** |
| 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. | [*Please insert relevant retention period and rationale behind that retention period*] |
|  |  |

* 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 (is 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.]* |
|  |  |

## Consultation

In carrying out this PIA, MU consulted with the following stakeholders:

|  |  |
| --- | --- |
| **Included Consultants** | **Feedback given** |
|  |  |

## Contact

**E-mail**: [ann.mckeon@mu.ie](mailto:ann.mckeon@mu.ie)

**Telephone**: +353 1 7086184

**Postal Address**:

Data Protection Officer,

Maynooth University,

Room 17,

Humanity House

Maynooth

County Kildare.

Further information is available on the University web: <https://www.maynoothuniversity.ie/data-protection>

Maynooth University

Data Protection Office

Maynooth, Co. Kildare, Ireland.

**T** +353 1 708 6184 **E** ann.mckeon@mu.ie **W** maynoothuniversity.ie

1. [↑](#footnote-ref-1)