**Data Protection Risk Assessment**

**Template**

|  |  |
| --- | --- |
| **Project Name:** | **Date:** |
| **Project Owner:** | **Site:** |
| **Email address:** | **Phone Number:** |

# Template Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Date** | **Author** | **Comments** |
| 2.0 | May 2019 | TCD DPO |  |

# Risk Assessment Circulation

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reviewed/Consulted** |
| **Project Manager Details** | [Insert Date] | *Reviewed/Consulted* |
| **Other Details** | [Insert Date] | *Reviewed/Consulted* |
| **DPO Details** | [Insert Date] | *Reviewed/Consulted* |

Contents

[Template Version Control 1](#_Toc11161809)

[Risk Assessment Circulation 1](#_Toc11161810)

[Risk Assessment - Objective 3](#_Toc11161811)

[Instructions 3](#_Toc11161812)

[Examples 4](#_Toc11161813)

[Project Details 5](#_Toc11161814)

[Screening Questions 6](#_Toc11161815)

[Personal Data 8](#_Toc11161816)

[Lawful Basis – Ordinary Personal Data 8](#_Toc11161817)

[Lawful Basis – Sensitive Personal Data 9](#_Toc11161818)

[International Data Transfers 10](#_Toc11161819)

[Data Retention 10](#_Toc11161820)

[Data Subject Rights 11](#_Toc11161821)

[Training 11](#_Toc11161822)

[Processing Risks 12](#_Toc11161823)

# Risk Assessment - Objective

In line with the risk-based approach to data processing of the GDPR, carrying out a Data Protection Impact Assessment (DPIA) is not necessary for every processing operation. Instead, a DPIA is only mandatory where a type of processing is “*likely to result in a high risk to the rights and freedoms of natural persons*”.

The Article 29 Working Party, consisting of the representatives from each data protection authority in the EU, has adopted guidelines on DPIAs and whether processing is likely to result in a high risk for the purposes of the GDPR. The guidelines are available [here](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236).

The Office of the Data Protection Commission has provided detailed information on DPIAs, available [here](https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#identifying-whether-a-dpia-is-required).

Not all processing activities will require a DPIA to be undertaken. It is recommended therefore that you review the examples listed below and answer the screening questions to determine if a DPIA will be necessary. In cases where it is not clear whether a DPIA is required, the Trinity College Data Protection Unit recommends that a DPIA is carried out, as it is a useful process to determine risks and support compliance with data protection law.

**It is important to note that a DPIA is required as standard for research studies conducted at St. James’s Hospital, Tallaght University Hospital and all clinical sites in which Trinity researchers are active.**

If you require further assistance or advice you should contact the relevant Data Protection Officer:

Trinity College: [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie)

St James’s Hospital: [research@stjames.ie](mailto:research@stjames.ie)

Tallaght University Hospital: [dpo@tuh.ie](mailto:dpo@tuh.ie)

# Instructions

You should complete all of the questions in this template and forward the completed document to the Unit to receive feedback on any risks identified and recommendations on the actions or controls needed to address those risks.

It is the responsibility of the School or Business Unit Project Manager as the ultimate risk owner to ensure that the required controls are put in place and to sign off on any risks arising from the processing.

The Risk Assessment should be updated when appropriate to reflect any material changes to the processing as the Project progresses.

Examples

The following examples should be used to assess whether a particular processing operation requires a DPIA:

|  |  |  |
| --- | --- | --- |
| **Examples of processing** | **Possible Relevant criteria** | **DPIA likely to be required?** |
| A hospital processing patients’ genetic and health data via the hospital information system. | * Sensitive personal data or data of a highly confidential nature. * Data concerning vulnerable data subjects. * Personal data processed on a large scale. | Yes |
| Storage for archiving purposes of pseudonymised sensitive personal data concerning vulnerable data subjects involved in research projects or clinical trials. | * Sensitive personal data. * Data concerning vulnerable data subjects. * Possibly prevents data subjects from exercising a right or using a service or a contract. | Yes |
| An organisation systematically monitoring its employees’ activities, including the monitoring of the employees’ workstations, Internet activity etc. | * Systematic monitoring of individuals on a large scale. * Potentially excessive or unlawful processing of personal data. * Data concerning vulnerable data subjects. | Yes |
| The gathering of public Social Media data for generating profiles. | * Evaluation or scoring. * Data processed on a large scale. * Matching or combining of datasets. * Sensitive personal data or data of a confidential nature. | Yes |
| Processing of personal data from patients or clients by an individual physician, other healthcare professional or solicitor. | * Sensitive personal data or data of a highly personal/confidential nature. * Data concerning vulnerable data subjects. | No |

# Project Details

|  |  |
| --- | --- |
| **Project name** |  |
| **Project owner(s)** |  |
| **Project start date** |  |
| **Number of individuals whose personal data will be processed** |  |
| **IT systems used** |  |
| **Third parties involved**  **(Provide details including information on the contractual arrangements in place and confirm what due diligence has been carried out)** |  |

|  |
| --- |
| Description of Project |
| [INSERT DETAILS HERE – MAX 300 WORDS] |

Screening Questions

Note: Each screening question should be answered, and you should add any additional, relevant question(s) dependant on the risk and/or processing operation(s) you are assessing. These screening questions will help you to identify if a DPIA is required and provide valuable insight into the processing operation risks and areas to focus on.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Screening Question** | **Yes** | **No** | **N/A** | **Notes** |
| Does the processing require systematic and/or extensive evaluation *(via automated means*) of personal aspects of an individual(s)? |  |  |  |  |
| Will decisions be based on such evaluations that are likely to produce legal effects, or equivalent effects concerning the individual(s) |  |  |  |  |
| Is the processing on a large scale and/or does it involve special categories of data (sensitive data)? |  |  |  |  |
| Is the processing on a large scale and does it involve data relating to criminal convictions and offences? |  |  |  |  |
| Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (i.e. CCTV) |  |  |  |  |
| Will the project involve the collection of new information about individuals? |  |  |  |  |
| Will the project compel individuals to provide information about themselves? |  |  |  |  |
| Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |  |  |  |  |
| **Screening Question** | **Yes** | **No** | **N/A** | **Notes** |
| Is the information about individuals likely to raise high risk privacy concerns or expectations? |  |  |  |  |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place? |  |  |  |  |
| Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive? |  |  |  |  |
| Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them? |  |  |  |  |
| Will the project require you to contact individuals in ways which they may find intrusive? |  |  |  |  |
| Will any of the processing activities make it difficult for the data subject(s) to exercise their rights? |  |  |  |  |
| Will the operation involve processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects? |  |  |  |  |
| Will the processing involve individuals who are considered ‘vulnerable’? |  |  |  |  |
| Does the processing operation involve any significant risk of the personal information being leaked or accessed externally? |  |  |  |  |

# Personal Data

List the types of personal data that will be collected, used, accessed or shared for the purpose of the Project.

|  |  |  |
| --- | --- | --- |
| **Data Collected** | **Justification** | **Processing Activity** |
| *EXAMPLE: Participant names* | *Identification, so that we can apply matching codes across longitudinal data sets.* | *Excel database, situated in ‘X’ Drive on ‘X’ desktop computer at ‘X’ site.* |
| *EXAMPLE: Written consent* | *Legal basis for processing.* | *Paper forms, stored in locked filing cabinet at ‘X’ site. Access restricted to [detail] only.* |
|  |  |  |
|  |  |  |
|  |  |  |

# Lawful Basis – Ordinary Personal Data

If processing ‘Ordinary’ personal data then you must satisfy at least one of the lawful bases as set out under [Article 6 GDPR](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1):

|  |  |
| --- | --- |
| Consent |  |
| Performance of a contract |  |
| Legal obligation |  |
| Public interest or exercise of official authority |  |
| Vital interests of data subjects |  |
| Legitimate interests |  |

If using *Consent*, then describe the consent process and attach supporting documentation.

# Lawful Basis – Sensitive Personal Data

Sensitive personal data is defined as:

* Processing of personal data revealing
* racial origin
* ethnic origin
* political opinions
* religious beliefs
* philosophical beliefs
* trade-union membership
* Processing of genetic data for the purpose of uniquely identifying a natural person
* Processing of biometric data for the purpose of uniquely identifying a natural person
* Data concerning health
* Data concerning a natural person's sex life
* Data concerning a natural person’s sexual orientation

If processing sensitive personal data then, in addition to the Article 6 lawful basis, you must also satisfy one of the conditions as set out under [Article 9 GDPR](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1):

|  |  |
| --- | --- |
| Explicit Consent |  |
| Employment / DSP rights |  |
| Vital Interests of the data subject or another person |  |
| Carried out (internally) by a not-for-profit organisation |  |
| Information that has been already made public by data subject |  |
| Necessary for the establishment, exercise or defence of legal claims |  |
| Necessary for substantial public interest |  |
| Necessary for the provision of medical care/ administration |  |
| Necessary for reasons of public interest in the area of public health |  |
| Archiving purposes in the public interest/ Scientific or Historical Research purposes/ Statistical purposes |  |

If using *Explicit Consent*, then describe the consent process and attach supporting documentation.

# International Data Transfers

Will the data be transferred or stored outside the EEA at any point or placed with Cloud providers that store data outside the EEA? Provide details.

|  |
| --- |
| Description of data transfers |
| [INSERT DETAILS HERE] |

If you are transferring personal data outside of the EEA have you ensured that suitable conditions for transferring the data are in place? Provide details or state if unsure:

|  |  |
| --- | --- |
| Adequate jurisdiction |  |
| US Privacy Shield |  |
| Standard Contract Clauses |  |
| Binding Corporate Rules |  |
| Authorisation from the Data Protection Commission |  |
| Unsure |  |

# Data Retention

How long will the data be retained for and why? Provide details.

|  |
| --- |
| Data retention |
| [INSERT DETAILS HERE] |

# Data Subject Rights

What plans are in place for responding to a request from an individual in relation to their data protection rights?

These include:

* right of access;
* right to rectification;
* right to erasure;
* right to object to processing based on legitimate or public interest;
* right to data portability;
* right to object to profiling or making decisions about individuals by automated means.

|  |
| --- |
| Data Subject rights requests |
| [INSERT DETAILS HERE] |

# Training

What guidance and training will be provided to individuals involved in this project or activity to enable them to understand their data protection responsibilities? Provide details.

|  |
| --- |
| Data protection training |
| [INSERT DETAILS HERE] |

# Processing Risks

Describe the source of risk and nature of potential impact on individuals. Include associated Compliance and Corporate risks as necessary.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk detail** | **Risk rating (High, medium, low)** | **Solutions/Mitigating Actions** | **Effect** | **Outcome** | **Measure approved** |
| *Hacking into computers where project data is stored.* | *Low* | *All computers storing data are password protected. The external hard drive and remotely accessible computer are also encrypted and locked in an office (on Trinity’s campus). Access is restricted to designated staff only.* | *Reduced* | *Low* | *Yes/No* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |