**Data Protection Risk Assessment (DPRA)**

**Template - Research**

|  |  |
| --- | --- |
| **Research Study / Project (‘Study’) Title:** | **Date:** |
| **Completed by:** | **Location:** |
| **Email:** | **Phone Number:** |

# DPRA Circulation

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reviewed/Consulted** |
| **Principle Investigator (PI) Details** | [Insert Date] | Reviewed/Consulted |
| **Co-I/Other Details** | [Insert Date] | Reviewed/Consulted |
| **DPO Details** | [Insert Date] | Reviewed/Consulted |

# DPRA - 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). Further information is available at [www.tcd.ie/dataprotection](http://www.tcd.ie/dataprotection).

Not all processing activities will require a DPIA to be undertaken. It is recommended therefore that you review the examples listed on the pages below and answer the screening questions to determine if a DPIA will be necessary. If a DPIA is required, then please use the relevant DPIA template instead (Health or Non-Health research as appropriate) - available at:

<https://www.tcd.ie/dataprotection/trinitycollegetemplates/>.

In cases where it is not clear whether a DPIA is required, the Trinity College Data Protection Office 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 relevant DPO 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 PI 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 DPRA should be updated when appropriate to reflect any material changes to the processing as the study progresses.

DPIA required?

The following questions should be reviewed to assess whether a particular processing operation requires a DPIA. If the answer is ‘yes’ to **two** of the questions below then please complete the relevant DPIA template.

|  |  |
| --- | --- |
| **Question** | **Yes / No** |
| Does the project involve matching or combining datasets? | Y / N |
| Are the topics explored in the project particularly intrusive or sensitive in nature? | Y / N |
| Does the project use personal data on a large scale for a purpose other than that for which was initially collected? | Y / N |
| Does the project involve the use of information about hospital patients? | Y / N |
| Does the project involve the use of genetic data? | Y / N |
| Are the participants individuals with a rare disease? | Y / N |
| Does the project involve the use of new technologies which are likely to result in a high risk to the privacy rights of research participants? | Y / N |
| Does the project involve large-scale processing of special category data or data relating to criminal convictions and/or offences? | Y / N |
| Does the project involve systematic monitoring, tracking or observing individuals' location or behaviour? | Y / N |
| Could the project result in decisions being made or actions being taking against individual(s), in ways that could have a significant impact on them? | Y / N |
| Does the project involve the use of profiling or algorithmic or special category data which could have a legal or similarly significant effect on the individual or is on a large scale? | Y / N |
| Could the project prevent individuals from exercising a right, using a service or fulfilling a contract? | Y / N |

# 

# Study Details

|  |  |
| --- | --- |
| Study name |  |
| Study owner(s) |  |
| Study 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 Study |
| [INSERT DETAILS HERE – MAX 300 WORDS] |

# Personal Data

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

|  |  |  |
| --- | --- | --- |
| **Data Collected** | **Justification** | **Processing Activity** |
| EXAMPLE:  Participant names | EXAMPLE:  Identification, so that we can apply matching codes across longitudinal data sets. | EXAMPLE:  Excel database, situated in ‘X’ Drive on ‘X’ desktop computer at ‘X’ site. |
| EXAMPLE:  Written consent | EXAMPLE:  Evidence of consent obtained from participants to meet legal requirements. | EXAMPLE:  Paper forms, stored in locked filing cabinet at ‘X’ site. Access restricted to [detail] only. |
| EXAMPLE:  Data concerning health |  |  |
| EXAMPLE:  Photos, video / audio recorded interviews which could identify the person |  |  |
| EXAMPLE:  Location data |  |  |
| EXAMPLE:  Information relating to the family of the individual and the individual’s lifestyle and social circumstances |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Transparency of Processing

Describe how you will you ensure that individuals are suitably informed of the intended processing and their rights under GDPR. This is a legal requirement under GDPR and must be correctly implemented.

Attach relevant Privacy Notices, Privacy Policies, Data Protection Statements, introductory emails to participants etc. **Attach supporting documents**, including Consent Form(s) and Participant Information Leaflet(s). These must be provided as part of the DPRA review process. The approved Trinity College templates must be used to ensure compliance with GDPR and the Data Protection Acts. These can be downloaded at: <https://www.tcd.ie/dataprotection/trinitycollegetemplates/>

# Data Security

1. Please provide a detailed description of the technical and organisational security measures in place to keep project data secure for each system, platform and application you will use for access, storage, and transfer, including but not limited to: **multi factor authentication, use of passwords, use of VPN, device encryption, access controls, vendor ISO certification, anti-virus used, use of secure file transfers such as HEAnet, detail on how data is backed up etc.** **Confirm what IT due diligence you have carried out (to include how data is backed up, managed and kept secure).**
2. Have you familiarised yourself with the Trinity College [Personal Data Breach Procedural Guidelines](https://www.tcd.ie/dataprotection/databreach/)?
3. Have you completed Data Protection training?

|  |
| --- |
| Data Security |
| [INSERT DETAIL HERE] |

# Purpose Limitation

Is the processing for the intended purpose only, or is there possibility that additional purposes may be added at a later date? You must ensure that ‘function creep’ is avoided.

|  |
| --- |
| Purpose Limitation |
| [INSERT DETAIL HERE] |

# Data Minimisation

Have you ensured that you will only collect the minimum data that you need or that is necessary for the activity? Provide details.

|  |
| --- |
| Data Minimisation |
| [INSERT DETAIL HERE] |

# 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.

# Data Sharing

Will the data be shared with third parties? If so, provide details including information on the contractual arrangements in place and confirm what due diligence has been carried out.

This list should include all Data Processing and Data Sharing Agreements, SLAs and MOUs with external parties, Cloud-based Solutions Agreements, Material Transfer Agreements etc.

|  |
| --- |
| Data Sharing |
| [INSERT DETAIL HERE] |

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. 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 |  |
| Standard Contract Clauses |  |
| Binding Corporate Rules |  |
| Authorisation from the Data Protection Commission |  |
| Unsure |  |

# 

# 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 |
| [INSERT DETAIL HERE] |

# Data Quality

How will the data be kept accurate, consistent and up-to-date?

|  |
| --- |
| Data Quality |
| [INSERT DETAIL HERE] |

# Data Retention

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

2. How will personal data be fully anonymised or destroyed after it is no longer necessary?

|  |
| --- |
| Data Retention |
| [INSERT DETAIL HERE] |

# Processing Risks - Examples

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

Examples of privacy risks that might be applicable:

**Risks to individuals**

* Hacking of computers where study data is stored.
* The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
* New surveillance methods may be an unjustified intrusion on their privacy.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
* Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
* Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
* If a retention period is not established information might be used for longer than necessary.

**Compliance risks**

* Non-compliance with the common law duty of confidentiality
* Non-compliance with the Data Protection Acts 2018/ General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations (PECR)/ e-Privacy Regulation.

**Associated organisation/corporate risks**

* Non-compliance with the data protection or other legislation can lead to sanctions, fines and reputational damage.
* Problems which are only identified after the project has launched are more likely to require expensive fixes.
* The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
* Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
* Data losses which damage individuals could lead to claims for compensation.

Different projects carry different risks and these should be considered. The above examples are a guide, not an exhaustive list.

# Processing Risks

Describe the source of risk and nature of potential impact on individuals as well as implemented or suggested solutions / mitigating actions.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk detail** | **Risk rating (High, medium, low)** | **Solutions/Mitigating Actions** | **Effect** | **Outcome** | **Measure approved by DPO** |
| *EXAMPLE*  *Hacking into computers where project data is stored.* | *EXAMPLE*  *High* | *EXAMPLE*  *All computers storing data will be password protected. The external hard drive and remotely accessible computer will be encrypted and locked in an office on Trinity’s campus. Access is restricted to designated staff only.* | *EXAMPLE*  *Reduced* | *EXAMPLE*  *Low* | *EXAMPLE*  *Yes* |
| *EXAMPLE*  *If a retention period is not established information might be used for longer than necessary.* |  | *All relevant data will be saved electronically, held in confidence and stored in secure password-protected computers. All the electronic documents will be deleted and destroyed after a period of [INSERT] months / years in accordance with standard University procedures.* |  |  |  |
| *EXAMPLE*  *Information which is collected and stored unnecessarily, or is not properly managed, so that duplicate records are created, presents a greater security risk.* |  | *All digital files (all data collected during the project) in an external hard drive computer. A back-up copy of files will be retained on OneDrive cloud storage platform. A single file (Excel format) linking the codes to data subjects will be encrypted (using 256-bit keys (AES-256) encryption software) and will be held by the project owner.* |  |  |  |
| *EXAMPLE*  *Non-compliance with the common law duty of confidentiality.* |  | *Information and consent forms will explicitly inform participants that their data will be kept confidential, but will emphasise the statutory limitations of confidentiality. Confidentiality may be breached in circumstances in which the research team has a strong belief or evidence exists that there is a serious risk of harm or danger to either the participant or another person. Disclosure may be required as part of a legal process or Garda investigation. In such instances, information may be disclosed to significant others or appropriate third parties without permission being sought from the participant. Where possible, a full explanation will be given to the participant regarding the necessary procedures and also the intended actions that may need to be taken.* |  |  |  |
| *EXAMPLE*  *The context in which information is used or disclosed can change over time, leading to it being used for different purposes without participant’s knowledge.* |  | *Participant’s data will not be subject to further processing that is incompatible with the purpose of the present study.*  *Privacy notice will make participants aware of how data is processed.* |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |