**Data Protection Impact Assessment (‘DPIA’) - Services**

|  |  |
| --- | --- |
| **Project / System / Product / App / Process (‘Project’):** | **Date:** |
| **Completed by:** | **Area / School / Department:** |

# DPIA Circulation

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reviewed/Consulted** |
| **Project Owner** | [Insert Date] | Reviewed/Consulted |
| **Project Manager** | [Insert Date] | Reviewed/Consulted |
| **Data Protection Officer** | [Insert Date] | Reviewed/Consulted |

DPIA - Objective

The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation.

The DPIA methodology provides evidence that risks to individuals have been considered and sufficient measures have been taken to protect those individuals.

The DPIA should measure the processing activity to be carried out against each of the Principles of data protection and determine whether the processing of personal data for the purposes of the Project is both necessary and proportionate or whether changes to the process or additional controls are required.

DPIA - Instructions

You should complete all of the section in this template and forward the completed document to the DPO at [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie) to receive feedback on any risks identified and recommendations on the actions or controls needed to address those risks.

If you are completing a DPIA for Research (either Health or non-Health related research) **do not use this template**. Instead, please use one of the relevant templates which are available to download at: <https://www.tcd.ie/dataprotection/research/>.

It is the **responsibility of the Project Owner** to ensure the required controls are put in place and to sign off on any risks arising from the processing.

The DPIA should be updated to reflect any material changes to the processing as the Project progresses.

All Trinity-controlled personal data, including data processed using third party systems, must be processed in compliance with the University’s [Data Protection Policy](https://www.tcd.ie/media/tcd/about/policies/pdfs/Data-Protection-Policy-16122020.pdf), [IT and Cyber Security Policy](https://www.tcd.ie/media/tcd/about/policies/pdfs/IT-and-Cyber-Security-Policy.pdf), and [Cloud Computing Policy and Guidelines](https://www.tcd.ie/about/policies/assets/pdf/Cloud-Policy-2014-final.pdf) (if appropriate).

# Introduction

|  |
| --- |
| **Provide a summary overview of the Project.** |
| Insert detail |

# Project Details

|  |
| --- |
| Number of individuals whose personal data will be processed as a result of the Project |
| Insert detail |
| Why is the use of [personal data](https://gdpr-info.eu/art-4-gdpr/) (i.e. data relating to an identifiable individual) necessary for the Project? |
| Insert detail |
| Description of personal data that will be collected, used, accessed, retained or shared (internal and external of Trinity College) for the purpose of the Project  EXAMPLE:  Name, address, D.O.B., age, gender, mobile number, email address, other |
| Insert detail |
| List the types of [sensitive personal data](https://gdpr-info.eu/art-9-gdpr/) (e.g. health data) or confidential data (e.g. financial data) that will be collected, used, accessed or shared for the purpose of the Project  See <https://www.tcd.ie/itservices/keeping-it-secure/data-classification/> for further information. |
| Insert detail |
| How is the personal data processed?  Describe the processing operations, including the *source of the data* and *scope, duration and purposes* of the processing.  Attach relevant data flowcharts *and* data maps *if available* from source to archive/destruction, records of processing activities etc. which clearly explain the internal and external data pathways. |
| Insert detail |
| Systems, software, platforms, hardware, formats involved |
| Insert detail |
| List the Parties involved  Include internal stakeholders, collaborators, external organisations (public/private), third party service providers, contractors, partners etc. |
| Insert detail |
| Does the Project involve matching or combining datasets? |
| Insert detail |
| Does the Project involve processing data concerning vulnerable individuals or where there may be an imbalance between the data subject and Trinity College (such as employees, patients etc.)? |
| Insert detail |
| Does the activity involve new, or innovative uses of technological or organisational solutions? |
| Insert detail |
| Could the activity prevent individuals from exercising a right, using a service or fulfilling a contract? |
| Insert detail |
| Is the use of the personal data being used in whole or part for a different purpose than the original purpose for which it was collected (secondary use)? |
| Insert detail |
| Does the activity involve data concerning children (anyone under 18)? |
| Insert detail |
| Other relevant information |
| Insert detail |

# Necessity & Proportionality

|  |
| --- |
| Are all the listed items required or could they be removed without compromising the Project’s goals?  There must be justification for processing the data. Processing of personal data constitutes a limitation on the right to the protection of personal data and must comply with EU law.  This requires ensuring that the processing of data as part of the Project is both necessary and proportional and has minimal impact on individuals’ rights and freedoms. |
| Insert detail |

# Legal Basis for Processing

|  |  |
| --- | --- |
| This is the valid legal reason for processing  If processing 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 |  |

# Lawful Basis – Special Category Data (Sensitive Personal Data)

|  |  |
| --- | --- |
| If processing special categories of personal data, the Project must 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) in addition to the Article 6 lawful basis | |
| 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 |  |

# Transparency of Processing

|  |
| --- |
| **Describe how affected 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** |
| Insert detail |

# 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 should ensure that ‘function creep’ is avoided** |
| Insert detail |

# Data Minimisation

|  |
| --- |
| **Have you ensured that you will only collect the minimum data that you need or that is necessary for the Project?** |
| Insert detail |

# Data Quality

|  |
| --- |
| **How will the data be kept accurate and up to date?****Are you able to amend information when and where necessary to ensure currency and accuracy of personal data processed as part of the Project and its applications?** |
| Insert detail |

# Data Security and Integrity

|  |  |
| --- | --- |
| Who is responsible for Project administration? |  |
| Describe in detail the technical and organisational security measures in place which will be taken to protect Project data, including but not limited to encryption, vendor ISO certification, anti-virus used etc. |  |
| Does the system processing the personal data have access controls (E.g. role-based, location-based, time-based access)? |  |
| If role-based controls, outline respective roles and responsibilities. |  |
| Describe how the effectiveness and adequacy of privacy controls are monitored. |  |
| If location-based access, how is physical access controlled? |  |
| Are copies of the data made and retained? If so, describe. |  |
| Confirm that all accounts created on relevant software systems have passwords configured which comply with the Trinity [Password Policy](https://www.tcd.ie/media/tcd/about/policies/pdfs/IT-and-Cyber-Security-Policy.pdf). Minimum of 10 characters, mixture of upper lowercase and special characters. |  |
| Describe how events are logged and how long this log is retained. |  |
| Monitoring of software, hardware, relevant IT networks. Describe process. |  |
| Describe how backups are managed and kept secure. |  |
| Does the vendor company have an IT Security / Privacy Policy and Privacy Notice / Data Protection Statement? If so, please attach. |  |
| Provide links to policies, procedures etc. relevant to the Project.  Please provide any additional information or documentation which can provide the University with an assurance that Project data is secure. |  |
| Have you familiarised yourself with the Trinity College Personal Data Breach [Procedural Guidelines](https://www.tcd.ie/dataprotection/assets/docs/databreach/TCD_Data_Breach_Procedural_Guidelines_052021.docx)? |  |

# Data Subject Rights

|  |
| --- |
| **What plans are in place for responding to a request from an individual in relation to their data protection rights?** **right of access****right to rectification****right to erasure****right to object to processing****right to data portability****right to object to profiling or making decisions about individuals by automated means** |
| Insert detail |

# Data Retention and Destruction

|  |
| --- |
| **How long will the data be retained for and why?** **How will data be pseudonymised, anonymised or destroyed after it is no longer necessary?****Describe archiving process.****Describe deletion / destruction process.** |
| Insert detail |

# Agreements

|  |
| --- |
| 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.  Contact [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie) for assistance.  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. |
| Insert detail |

# International Data Transfers

|  |
| --- |
| **Will the data be transferred or stored outside the UK or European Economic Area (‘EEA’) at any point or placed with Cloud providers that store data outside the UK or EEA?** **If transferring personal data outside the UK or EEA, are suitable conditions in accordance with** [**Chapter V GDPR**](https://gdpr-info.eu/chapter-5/) **requirements for transferring the data are in place?** **Provide details or state if unsure.****Suitable conditions:****Adequate jurisdiction****Standard Contract Clauses** **Transfer Impact Assessment****Authorisation from the Data Protection Commission** |
| Insert detail |

# Training

|  |
| --- |
| **The provision of training in data protection law and practice is a mandatory requirement for Trinity College staff.** **What guidance and training will be provided to the staff, contractors and students involved in the Project to enable them to understand their data protection and IT security responsibilities?****Trinity College – KnowBe4 online Data Protection and Cybersecurit**y **training module available at:**[**https://www.tcd.ie/dataprotection/training/**](https://www.tcd.ie/dataprotection/training/) |
| Insert detail |

# 

# Processing Risks - Examples

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

Include associated Compliance and Corporate risks as necessary. It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a ‘Likelihood’ and ‘Impact’ score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below.

**Risks to individuals - Examples**

**Likelihood**

**Impact**

1 - Rare

2 - Unlikely

3 - Possible

4 - Likely

5 - Highly Likely

1 - Negligible

2 - Minor

3 - Moderate

4 - Major

5 - Critical

5

4

9

20

15

12

10

16

8

4

2

1

4

3

2

5

6

8

3

10

6

15

20

12

25

* Hacking of computers where Project 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.
* Incorrect or overuse of individuals’ data.
* Lack of transparency, fairness or lawfulness of processing activities.
* Failure to explain effectively how data would be used.
* 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.
* Anonymisation techniques chosen may turn out to be ineffective.
* Use of technology capable of making visual or audio recording may be unacceptably intrusive.
* 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 1988-2018/ General Data Protection Regulation (GDPR) 2016, Privacy and Electronic Communications Regulations (PECR), Universities Act 1997, HEA Act 2022 etc.

**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 Trinity College.
* Public distrust about how information is used can damage Trinity’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 - Table

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

**Include associated Compliance and Corporate risks as necessary.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risk detail | **Risk likelihood**  **(1 – 5)** | **Risk severity**  **(1 – 5)** | **Risk**  **score**  **(1 – 25)** | **Solutions / Mitigating Actions** | **Solutions / Mitigating actions implemented?** | **Residual risk**  **(Unchanged / Reduced / Eliminated)** | **New score** |
| *EXAMPLE*  *Breach of personal data held electronically as a result of a cyber-attack.* | *e.g.* ***4*** | *e.g.* ***5*** | *e.g.* ***20*** | ***EXAMPLE***  *All devices and systems processing project data will be encrypted and password protected using secure approved methods as appropriate.*  *Data is encrypted at rest using industry standard encryption techniques (e.g. AES).*  *Secure HTTPS communication using Transport Layer Security (TLS) / HEANet used for data transfers.*  *Approved College-controlled systems used to process project data only.*  *Access to project data (devices and software accounts) restricted to designated staff only. Access controls reviewed periodically.*  *Critical patches are applied to servers on a priority basis and as appropriate for all other patches.*  *Service provider maintains a documented vulnerability management program which includes periodic scans and penetration testing, identification and remediation of security vulnerabilities on servers, workstations, network equipment and applications.* | *Yes* | *Reduced* | *e.g.* ***12*** |
| *EXAMPLE*  *Retention periods are not established/followed. Data may be kept longer than required.* |  |  |  | ***EXAMPLE***  *Relevant project data will be deleted / archived / anonymised as appropriate after a period of [INSERT] months / years in accordance with University policy and best practice.* |  |  |  |
| *EXAMPLE*  *Data is not properly managed in line with Project deliverables. Duplicate records are created unnecessarily and present a greater security risk.* |  |  |  | ***EXAMPLE***  *Data to be retained in Project software team account and / or shared SharePoint / OneDrive / Teams site only to prevent data duplication. Data export from shared systems to be restricted except when necessary. Data will not be saved to hard drives. Attachments containing Project data will not be shared via email.* |  |  |  |
| *EXAMPLE*  *The context in which data is used or disclosed can change over time, leading to it being used for different purposes without relevant individuals’ knowledge.* |  |  |  | ***EXAMPLE***  *Individuals’ data will not be subject to further processing that is incompatible with the current purposes of the Project. Any further processing of relevant data will be subject to review in advance of processing.* |  |  |  |
| *EXAMPLE*  *Unnecessary or arbitrary disclosure of personal data internally within the University due to a lack of appropriate controls being in place.* |  |  |  | ***EXAMPLE***  *Access to Project data is restricted to designated staff only. Permissions settings have been configured to restrict access by default. Permissions to be reviewed periodically by Project owner.* |  |  |  |
| *EXAMPLE*  *Accidental loss of / theft of devices (Laptop, PC, Tablet, Phone, Server) may lead to risk of unauthorised disclosure of personal data to third parties.* |  |  |  | ***EXAMPLE***  *Devices used to process Project data are encrypted. Access to data is restricted to designated staff only. Access is via multifactor authentication.*  *Pseudonymisation implemented to mitigate risk associated with processing. Key code is kept separately to pseudonymised Project data to mitigate any inappropriate disclosure. Access to identifiable data items is restricted to limited members of Project team.* |  |  |  |
| *EXAMPLE*  *Information released / published / shared in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.* |  |  |  | ***EXAMPLE***  *Anonymisation techniques will follow DPO guidance and be kept under review prior to any data being disclosed.*  *IT Services Data Classification information to be taken into account:* [*https://www.tcd.ie/itservices/keeping-it-secure/data-classification/*](https://www.tcd.ie/itservices/keeping-it-secure/data-classification/) |  |  |  |
| *EXAMPLE*  *Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.* |  |  |  | ***EXAMPLE***  *Project owner to review any intended use of datasets in conjunction with other datasets on file at the University.* |  |  |  |
| *EXAMPLE*  *IT Services have not been consulted on software deployment.* |  |  |  | ***EXAMPLE***  *Project owner to engage with IT Services to ensure that data processing of University data is carried out in compliance with University policy.* |  |  |  |
| *EXAMPLE*  *Agreement with service provider / partner not in place / has not be reviewed for compliance with GDPR.* |  |  |  | ***EXAMPLE***  *Project owner to consult with DPO & College Solicitor’s office to get contract reviewed. Agreement to include GDPR Art. 28 clauses / appropriate JCA terms as appropriate.* |  |  |  |
| *EXAMPLE*  *Data may be transferred to countries with inadequate data protection regimes.* |  |  |  | ***EXAMPLE***  *Project data will not be transferred outside of the UK or EEA without consultation with the DPO’s office and appropriate mechanism being in place.* |  |  |  |
| *EXAMPLE*  *Software is using AI – possible loss of control over data / non-compliance with EU AI Act* |  |  |  | ***EXAMPLE***  *Project team has engaged with DPO / IT Services / College Solicitor / relevant College departments to address possible risks associated with AI inherent in Project software and impact on Project data.* |  |  |  |