**Data Protection Risk Assessment**

# **Instruction**

Please review / complete **all FIVE parts** of this document to provide detail on how and why [personal data](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en) will be processed for your research study and to determine if further assessment from the Trinity College Data Protection Office will be required. Please remember that data protection legislation, and this document, applies to the processing of ‘personal data’ (including pseudonymised personal data) only. Data protection law does not apply to anonymous data or irrevocably anonymised data. Further information is available [here](https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf).

You must return the completed document to the [Data Protection Office](mailto:dataprotection@tcd.ie) to receive feedback and instruction before you progress with your ethics application.

Transparency of Processing

*There are no exemptions under GDPR to transparency obligations towards participants*

Please attach your Participant Information Leaflet and Consent Form and any Invitation Letter, Debriefing Sheet, Privacy Notices, Privacy Policies, Data Protection Statements etc. that you have drafted. You must use the TCD-provided Participant Information Leaflet and Consent Form templates available [here](https://www.tcd.ie/dataprotection/trinitycollegetemplates/).

It is the responsibility of the Research Supervisor / Supervisor / Principal Investigator to ensure that information provided in this document is accurate and of sufficient quality to enable the DPO’s office to conduct an effective review.

**An incomplete document will be returned without review.**

# **Part 1 - Submission Information**

|  |  |  |
| --- | --- | --- |
| Title of study | (Provide detail) | |
| Trinity College School | (Provide detail) | |
| Date of submission | (Provide detail) | |
| Completed by | (Insert name) | |
| Supervisor / Principal Investigator (if not Researcher named above) | (Insert name) | |
| Email address | (Provide detail) | |
| Please tick **all** that apply. | Student Project  Masters  PhD | Staff Project  Funded  Non-Funded |
| Description of study | (Provide detail - maximum 300 words) | |

# **Part 2 - Data Protection Information**

|  |  |
| --- | --- |
| 1. Provide details of data protection training completed by research team members. Attach certificates of successful module completion | Research Integrity and Impact in an Open Scholarship Era (CA7000) module  RIO: Research Integrity and Impact in an Open Scholarship Era  Trinity College Data Protection Training (GDPR) Module - [Blackboard](https://www.tcd.ie/itservices/kb/vle/overview-GDPRtraining.php)  HSeLanD - Fundamentals of GDPR training  Other (provide detail) |
| 1. Are all researchers familiar with the Trinity College Personal Data Breach [Procedural Guidelines](https://www.tcd.ie/dataprotection/assets/docs/databreach/TCD_Data_Breach_Procedural_Guidelines_052021.docx)? | Yes  No |
| 1. Site of data collection | (Provide detail on any site where data will be collected or shared from) |
| 1. What is Trinity's [role](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en) in respect of the study? | Data controller  Joint data controller  Data processor |
| 1. If Trinity College is a joint data controller, provide detail of the other joint controllers and their Data Protection Officer contact details | (Provide detail) |
| 1. Number of individual participants, or anticipated numbers | (Provide estimated number) |
| 1. Type of participant (i.e. students, staff, patients, healthcare workers etc.) | (Provide detail) |
| 1. Is the study considered as [health research](https://www.tcd.ie/dataprotection/healthresearch/)? | Yes  No |
| 1. List the [personal data](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en) and /or [special category data](https://www.dataprotection.ie/en/organisations/know-your-obligations/lawful-processing/special-category-data) that will be processed for the study   *For example: Name, email address, interview recordings, transcripts, video recordings, health records, ethnicity, political beliefs, religion* | (Provide detail) |
| 1. How often will you need to collect data? | (Provide detail on frequency of data collection) |
| 1. Describe where and how the data will be processed / stored and if data will be shared internally   *For example: Cloud software (Trinity College Microsoft OneDrive, Teams, SharePoint), server in a data centre in Ireland, desktop / laptop of researcher (personal, College-issued), external hard drive / USB drive, paper files stored in secure room in hospital / office etc.* | (Provide detail - maximum 300 words) |
| 1. Provide a general description of the security measures in place to keep data secure.   *For example: Multi factor authentication, use of passwords, use of VPN, device encryption, vendor ISO certification, anti-virus used, use of secure file transfers such as HEAnet, detail on how data is backed up etc.* | (Provide detail - maximum 300 words) |
| 1. Is the data shared with any third-party organisation, including commercial entities? | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail.  *For example: the type of data being shared (description of the data), the reason for sharing, the format of the data that will be shared (i.e., whether identifiable, coded, or anonymous), the security measures in place to protect the data in transit and on receipt etc.*  *Specify if the third party is a data controller, data processor or joint controller(s).*  *Include data flowcharts if possible.* | |
| 1. Will the data be transferred outside of the UK & EEA? | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail on which country. Please name the organisation you are transferring to. | |
| 1. How long will the data be retained in an identifiable or coded format? | (Provide detail) |

# **Part 3 - DPIA Screening**

This section will help the College’s Data Protection Office to determine if your research project requires a [Data Protection Impact Assessment](https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=A%20Data%20Protection%20Impact%20Assessment%20(DPIA)%20describes%20a%20process%20designed,demonstrating%20compliance%20with%20the%20GDPR.) (‘DPIA’). The specific criteria listed below are those which are considered by the Data Protection Commission to represent a higher risk to individuals’ data protection and privacy rights. Please mark ‘Yes’ or ‘No’ for each of the following as listed.

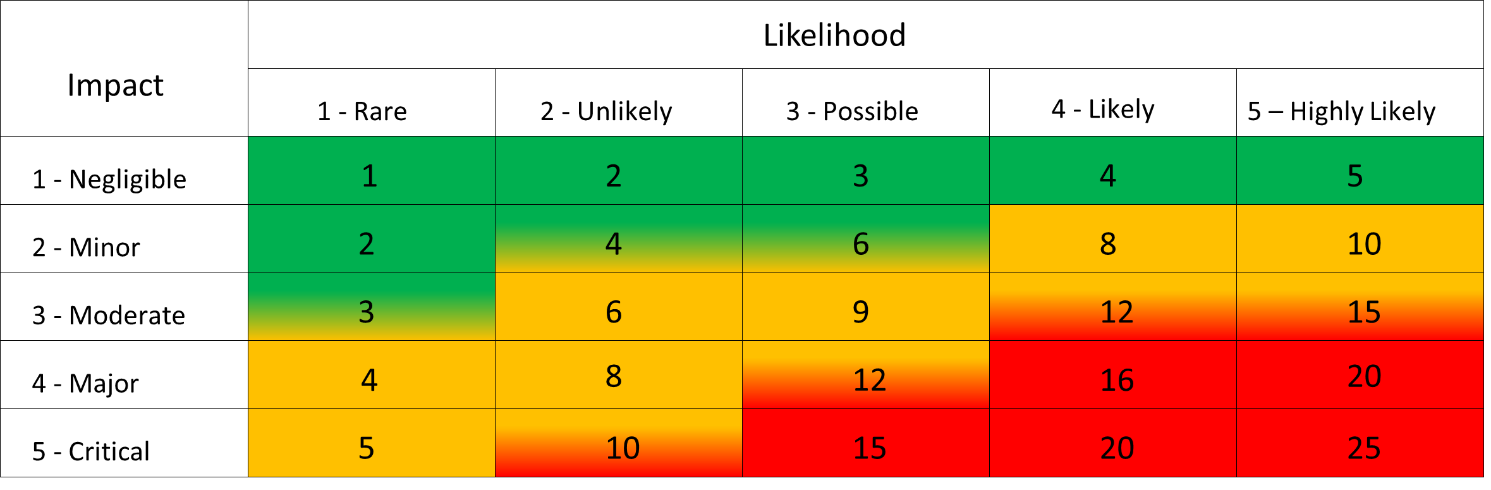
**Does your research involve any of the following:**

|  |  |
| --- | --- |
| 1. The use of [sensitive or special categories of data](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/). For example, data concerning a person’s health, genetic data, biometric data, ethnicity, political opinions, data concerning a natural person’s sex life or sexual orientation, data relating to criminal convictions. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. The secondary use of personal data e.g. information being taken from medical records or another database for use in a research project. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. The use of data concerning vulnerable individuals. For example, children (anyone under 18 years), employees, patients, people with an intellectual disability, the elderly, the mentally ill, asylum seekers, or in any case where a power imbalance in the relationship between the position of the participant and the researcher can be identified. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Topics that could be considered particularly intrusive or sensitive in nature. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Data processing on a large scale, either as a specific number or as a proportion of the relevant population, or due to the range of different data items needed, or due to the duration or longitudinal effect of the research, or where it occurs over a large geographical area. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Matching, linking, cross referencing or combining two or more separate datasets. For example, enriching datasets by using additional data sources to provide further information regarding the individuals in a research study. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Systematic monitoring, i.e., data processing to observe, monitor or control individuals, including data collected through systematic monitoring of a publicly accessible area. For example, collecting patient-related data at hospital level to understand bed occupancy, CCTV, GPS tracking etc. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Evaluation or scoring, including profiling individuals. For example, predicting outcomes in individuals based on their economic situation or performance at work, behaviours, health, preferences etc. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Automated decision-making which results in legal or similar significant effect. For example, a recruitment aptitude test which uses pre-programmed algorithms and criteria leading to the exclusion or discrimination of individuals etc. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Innovative use or application of new technological or organisational solutions. For example, machine learning, artificial intelligence, sentiment analysis etc. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |
| 1. Use of biometric data (fingerprint and face recognition, gait analysis) to uniquely identify an individual. | Yes  No |
| If you have answered ‘Yes’ to the previous question, provide further detail. | |

# **Part 4 -** **Processing Risks**

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 . 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

* 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.
* 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.
* Personal data being used for automated decision making may be seen as excessively 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 - examples

* Non-compliance with the common law duty of confidentiality.
* Non-compliance with the Data Protection Acts 1988- 2018 / General Data Protection Regulation (GDPR), Health Research Regulations 2018 (as amended), Privacy and Electronic Communications Regulations (PECR).

Associated organisation / corporate risks - examples

* Non-compliance with the data protection or other legislation can lead to sanctions, fines and reputational damage.
* Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
* Data breaches regarding privacy and personal data are likely to cause reputational risk to the University.
* Problems which are only identified after the study has commenced 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 a reluctance on the part of individuals to trust us, and to take part in our research projects.
* Data losses which damage individuals could lead to claims for compensation.
* Problems with data protection in the research project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
* Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
* Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against the University.

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

# **Part 5 - Processing Risks - Table**

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

Delete examples if not appropriate to your project and include any other risks that you have identified that are not included as examples.

Use the **RAG Matrix** above to help calculate the risk.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 data held electronically by hackers.* | *e.g. 4* | *e.g. 4* | *e.g. 16* | *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.* | *Yes* | *Reduced* | *e.g. 8* |
| *EXAMPLE*  *Data may be kept longer than required in the absence of appropriate policies.* |  |  |  | *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 study) 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.*  *PIL will make participants aware of how data is processed.* |  |  |  |
| *EXAMPLE*  *Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.* |  |  |  | *Access is restricted to designated staff only.*  *Only TCD approved systems will be used for sharing of information internally.* |  |  |  |
| *EXAMPLE*  *Accidental loss of electronic equipment by organisation’s personnel may lead to risk of disclosure of personal information to third parties.* |  |  |  | *Disaster recovery plan has been devised and implemented as part of the study design process.* |  |  |  |
| *EXAMPLE*  *Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.* |  |  |  | *All computers storing data will be encrypted. Access is restricted to designated staff only. Access is via 2FA. Key code is kept separately to research data to mitigate any inappropriate disclosure. Access is restricted to limited members of research team.* |  |  |  |
| *EXAMPLE*  *Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.* |  |  |  | *PIL will ensure that individuals are fully informed about how their information will be used.* |  |  |  |
| *EXAMPLE*  *Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out to be ineffective.* |  |  |  | *Anonymisation techniques will follow DPC guidance and be kept under review.* |  |  |  |
| *EXAMPLE*  *Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.* |  |  |  | *PIL will ensure that individuals are fully informed about how their information will be used.* |  |  |  |
| *EXAMPLE*  *Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.* |  |  |  | *Only information which is necessary for the research project will be collected.* |  |  |  |
| *EXAMPLE*  *Merging of datasets may inadvertently allow individuals to be identified from anonymised data.* |  |  |  | *Research team undertake not to seek to identify individuals if datasets are received from third parties.* |  |  |  |
| *EXAMPLE*  *Use of technology capable of making visual or audio recordings may be unacceptably intrusive.* |  |  |  | *Explicit consent to take part in visual and audio recording will be taken. Audio and/ or video is retained for minimal period of time until transcript is verified. Audio is then securely deleted.* |  |  |  |
| *EXAMPLE*  *Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.* |  |  |  | *Only minimal data is collected. All data is necessary for the project and has to be justified in the DPIA.* |  |  |  |
| *EXAMPLE*  *Data may be transferred to countries with inadequate data protection regimes.* |  |  |  | *No data will be transferred outside of EEA without consultation with the DPO’s office and appropriate mechanism being in place.* |  |  |  |