

# Data Protection Impact Assessment (DPIA) Template – Research

## Purpose of a DPIA

The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation. The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals. The DPIA should assess the activity to be carried out against all the principles of data protection and determine whether the processing of personal data is both necessary and proportionate or whether changes to the process or additional controls are required.

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 DDUH researchers are active. Each site will require its own DPIA.

<b>Study Name:</b>	<b>Date:</b>
<b>Owner:</b>	<b>Site:</b>
<b>Email:</b>	<b>Phone Number:</b>

## Template Version Control

Reference	Date	Author	Comments
1.0	June 2020	DDUH DPO	

## DPIA Circulation

Name	Date	Reviewed/Consulted
<b>PI Details</b>	[Insert Date]	<i>Reviewed/Consulted</i>
<b>Co-I/Other Details</b>	[Insert Date]	<i>Reviewed/Consulted</i>
<b>DPO Details</b>	[Insert Date]	<i>Reviewed/Consulted</i>

## Contents

Template Version Control .....	1
DPIA Circulation .....	1
Data Protection Checklist for Health Research.....	3
DPIA - Instructions .....	3
Study Details .....	4
Nature of Process/ System/ Project.....	4
Further details in respect of the intended processing .....	5
Any other information in respect of the study which may be relevant.....	5
Personal Data.....	6
Transparency of Processing .....	7
Data Security – Storage and Sharing .....	7
Data Minimisation.....	8
Lawful Basis – Ordinary Personal Data.....	8
Lawful Basis – Special Category Data (Sensitive Personal Data) .....	9
Health Research Regulations - Explicit Consent required for Health Research .....	10
High-Risk Processing.....	10
Internal Data Sharing .....	11
Third Parties .....	11
International Data Transfers .....	11
Data Retention .....	12
Data Subject Rights .....	12
Training.....	12
Processing Risks - Examples .....	13
Processing Risks - Table .....	14
Resources and Disclaimer.....	15

## Data Protection Checklist for Health Research

If your project relates to health research, then you must comply with the requirements of the [Health Research Regulations 2018](#).

You ***must*** carry out the following:

Obtain ethical approval for the health research by a research ethics committee. This must be granted prior to submission of the DPIA.	<input type="checkbox"/>
Identify and document the data controller, joint controllers and data processors.	<input type="checkbox"/>
Ensure relevant contractual arrangements are in place.	<input type="checkbox"/>
Identify and document funding bodies.	<input type="checkbox"/>
Identify third parties with whom data will be shared (even if pseudonymised) and for what purpose.	<input type="checkbox"/>
Ensure all members of the research team have completed data protection training.	<input type="checkbox"/>
Carry out a DPIA if the research represents a high risk to individuals or involves the use of genetic data, monitoring of behaviours, large scale processing of sensitive personal data, or involves data concerning vulnerable people (including children), use of the data for new purposes or the linking of datasets.	<input type="checkbox"/>
Ensure you only use the minimum data necessary to carry out the research.	<input type="checkbox"/>
Implement controls to ensure the integrity and accuracy of data and determine when the data has been altered, disclosed or erased and by whom.	<input type="checkbox"/>
Implement security measures to protect the personal data; e.g. device encryption.	<input type="checkbox"/>
Ensure the data is archived, anonymised or destroyed when the research is completed.	<input type="checkbox"/>
Ensure that participants are provided with sufficient information about the use of their personal data via Participant Information Leaflets, Consent Forms and the project website.	<input type="checkbox"/>
Obtain explicit consent for the processing of personal data for the health research including the screening of individuals for research purposes.	<input type="checkbox"/>

You should complete all of the questions in this template and forward the completed document to the data protection officer at [dataprotection@dental.tcd.ie](mailto:dataprotection@dental.tcd.ie) 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 Project Supervisor 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 or activity progresses.

## Study Details

### Nature of Process/ System/ Project

Describe in detail the nature of the process, system or project to be assessed.

Include:

- The **name** of the project.
- The **scope** of the processing.
- The **purpose** for the activity.
- The **frequency** of the processing.
- The **number of individuals** involved and/or affected.
- Details of the **parties and third parties** involved including other data controllers or processors.
- Details of any **systems** to be used.

### Nature of Process/ System/ Project

[INSERT DETAILS HERE – MAXIMUM 300 WORDS]

**Further details in respect of the intended processing**

Does the activity involve processing data on a large scale? If so, provide detail.	
Does the activity involve matching or combining datasets? If so, provide detail.	
Does the activity involve data concerning vulnerable individuals or children? If so, provide detail.	
Does the activity involve new, or innovative uses of, technological or organisational solutions? If so, provide detail.	
Could the activity prevent individuals from exercising a right, using a service, or fulfilling a contract? If so, provide detail.	
Why the use of personal data is necessary for this activity?	
Who will benefit from the activity?	
Could the use of the personal data for this activity result in any harm to the individual?	

**Any other information in respect of the study which may be relevant**

Additional information
<p>[INSERT DETAILS HERE – MAXIMUM 300 WORDS]</p>



### Transparency of Processing

How will you notify participants about the data processing that will be carried out using their personal data? Provide details and **attach copies** of the Consent Form(s) and Participant Information Leaflet(s).

#### Transparency of processing

[INSERT DETAILS HERE]

### Data Security – Storage and Sharing

Describe in detail the technical and organisational security measures which will be taken to protect personal data including but not limited to; access controls, data sharing restrictions, encryption, pseudonymisation, anonymisation etc.

#### Data security – storage and sharing

[INSERT DETAILS 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 DETAILS 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](#):

Consent	<input type="checkbox"/>
Performance of a contract	<input type="checkbox"/>
Legal obligation	<input type="checkbox"/>
Public interest or exercise of official authority	<input type="checkbox"/>
Vital interests of data subjects	<input type="checkbox"/>
Legitimate interests	<input type="checkbox"/>

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

### Lawful Basis – Special Category Data (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](#):

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

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

### Health Research Regulations - Explicit Consent required for Health Research

In addition to satisfying Articles 6 & 9 GDPR requirements you must also obtain explicit consent for processing personal data for health research purposes. This mandatory requirement is set out under Regulation 3(1) (e) of the [2018 Health Research Regulations](#).

Describe how you will ensure that explicit consent is obtained for processing personal data for health research purposes. **Attach supporting documents**, including Consent Forms and Participant Information Leaflets.

If you intend to seek a Public Interest Waiver from the Health Research Consent Declaration Committee (HRCDC) please review the *Pre-submission Checklist* which is available to download from the HRCDC [website](#) before proceeding further. If you require further assistance please contact the DDUH Data Protection Officer at [Data.protection@dental.tcd.ie](mailto:Data.protection@dental.tcd.ie)

#### Heath Research Regulations, Consent, Participant Information Leaflets

[INSERT DETAILS HERE]

### High-Risk Processing

Does the research involve any of the following?

- evaluating or predicting outcomes in individuals;
- decision making by automated means e.g. using algorithms;
- monitoring the behaviours of individuals;
- the surveillance of individuals, use of location or the use of biometric technology such as facial recognition.

If so, provide details and describe the impact to the individuals.

#### High risk processing

[INSERT DETAILS HERE]

### Internal Data Sharing

Will the data be shared internally? i.e. with departments or business units within the organisation? If so, provide details on the data sharing including information on the necessity for the processing, the format of the data that is to be shared, with whom the data will be shared and confirmation of the security measures in place to protect the data in transit.

#### Internal data sharing

[INSERT DETAILS HERE]

### Third Parties

Will the data be shared with third parties including IT service providers, Cloud-based solutions, sub-contractors etc.? If so, provide details including information on the contractual arrangements in place and confirm what due diligence has been carried out.

#### Third parties

[INSERT DETAILS HERE]

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

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

#### International data transfers

[INSERT DETAILS HERE]

### 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 subjects rights

[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.

#### Training

[INSERT DETAILS 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 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.
- 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.



**Resources and Bibliography:**

Data Protection Commissioner Guidance on Data Protection Impact Assessments (DPIAs)  
ICO Information Commissioner's Office UK  
Health Research Regulations 2018  
Trinity College Dublin, DPIA  
St. James's Hospital Dublin, DPIA  
University College Cork, DPIA

**Disclaimer**

**This material contained in this guidance contains general information and guidance only. Please note that this guidance does not constitute legal advice and is provided for general purposes only. Neither is it intended to provide a comprehensive or detailed statement of the law.**

**No liability whatsoever is accepted by the Dublin Dental University Hospital for any action taken in reliance on the information contained in this guidance. You should not act or refrain from acting, on the basis of any information provided in this guidance but rather you should always seek specific legal or other professional advice. Any and all information is subject to change without notice.**