

## **What is a DPIA?**

A DPIA is a way for you to systematically and comprehensively analyse processes and projects which involve the processing of personal data and help you to identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material, or non-material.

To assess the level of risk, a DPIA must consider both the likelihood of harm and the severity of any impact on individuals.

A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified

## **When should a DPIA be conducted?**

This DPIA report should be completed prior to the commencement of a process or project which involves the use of personal data.

## Table of Contents

Data Protection Impact Assessment Report .....	1
What is a DPIA?.....	1
When should a DPIA be conducted?.....	1
1. identify the need for a DPIA .....	3
2. Describe the processing.....	4
A. Data Map.....	5
B. Describe the purpose of the processing .....	6
C. Describe the nature of the processing .....	6
D. Describe the scope of the processing .....	6
E. Describe the context of the processing .....	7
F. Consultation Process .....	8
G. Necessity & Proportionality .....	9
H. Security .....	11
3. identify & Assess Risks .....	13
4. Risk Mitigation .....	19
5. Approval & Sign off .....	20
Appendix A – Principles of Data Protection .....	21
Appendix B –Privacy Risks .....	23
Appendix C – Assessing Risk .....	25

# 1. IDENTIFY THE NEED FOR A DPIA

Under the GDPR, DPIAs are mandatory for any new **high-risk** processing projects. The DPIA process allows organisations to make informed decisions about the acceptability of data protection risks and communicate effectively with the individuals affected.

Question	Answer
Project or process:	<p>The Fund for Student with Disabilities (FSD) participant data is processed by the HEA received from UK/EEA HEIs on behalf of Irish students studying there. The purpose of which is to provide funding for Irish students studying in those HEIs.</p> <p>FSD is funded by the Irish government through the HEA.</p> <p>The overall objective of FSD is to contribute to enhancing attainment of tertiary education qualifications by students with disabilities.</p>
Summary of processing:	<p>FSD Applications forms are submitted to the HEA by UK/EEA HEIs on behalf of Irish Students. The HEA then review the data and claims. The HEA reviews the submissions for completeness and compliance with the Guidelines, and assesses submissions for the purposes of allocating funding. Aggregated data are used for reporting and statistical purposes, and are shared with third parties/published.</p>
Why have you identified the need for a DPIA? Refer to risk assessment findings.	<p>The processing involves sensitive personal student data, including Special Category Data.</p>
Identify any associated documentation which is relevant to this DPIA.	<p>FSD EEA/UK Guidelines, issued on annual basis.</p> <p>Standard Data sharing agreement between the HEA and EEA/UK based HEIs participating in FSD.</p> <p>Internal standard operational procedures pertaining to administration of FSD.</p>

## 2. DESCRIBE THE PROCESSING

Describe how and why you plan to use the personal data. Your description must include **the purposes, nature, scope, and context of the processing.**

Documentation received are saved in the relevant institutional folder on the shared drive as files and relevant emails which need to be retained are saved into a subfolder. Only authorised HEA staff members who are participating in the administration of FSD have access to the relevant folders on the shared drive.

The following preliminary checks are carried out by the HEA to ensure:

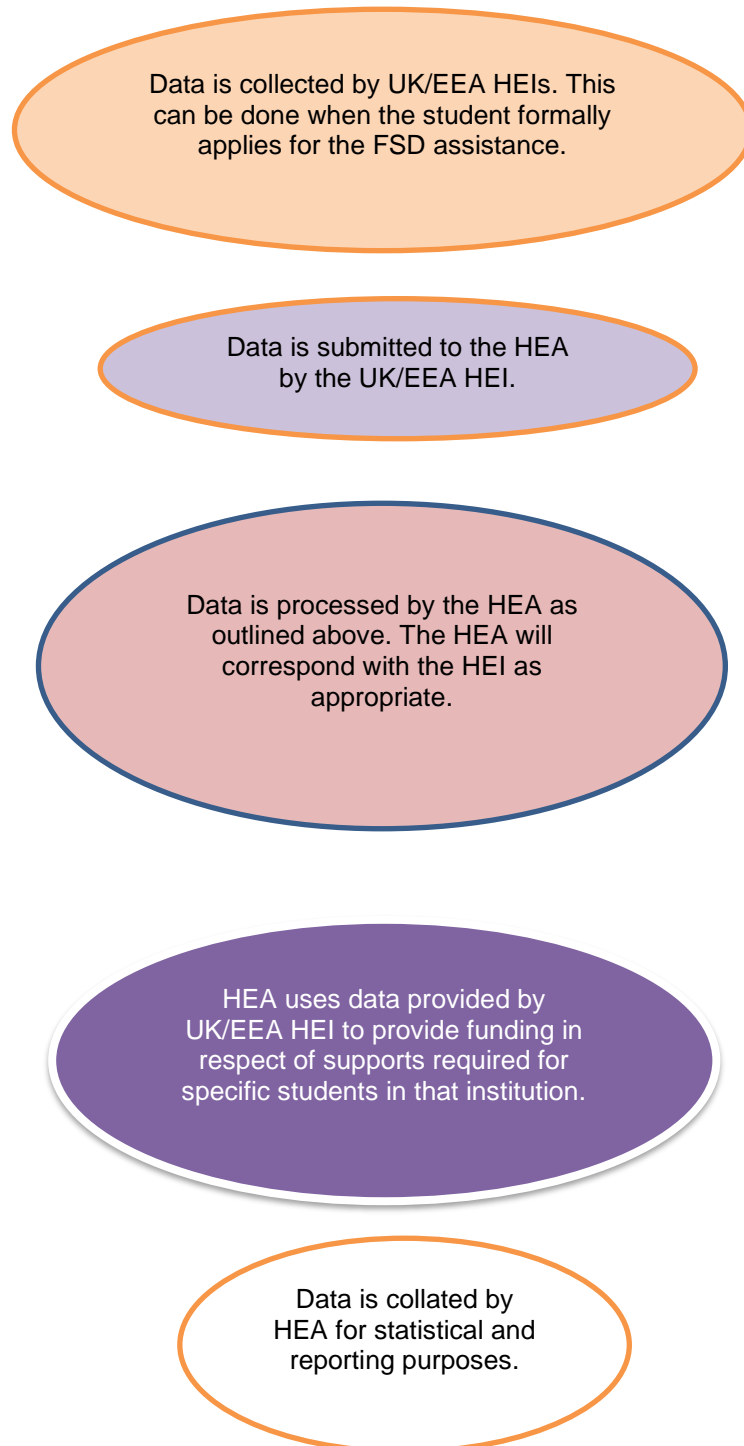
1. All required fields are completed, i.e., personal information, residency question, course information, supports requested.
2. Student, course, and institution are eligible for FSD funding.
3. Supports requested are eligible for FSD expenditure.
4. The various supporting evidence provided is consistent with the information included in the application form, such as disability and supports needed.
5. Application form is signed and dated by the disability officer and the student declaration is signed and dated.

If the application does not pass any of the above checks, the HEA emails the relevant disability officer and requests that issues identified are rectified. If an application is deemed ineligible at this stage, the HEA notifies the disability officer.

The assessment of applications for the purposes of allocation of funding involves participation of HEA Access Policy section. Following determination of allocations in respect of individual students, HEIs are notified of the outcome of the process and funding is transferred by the HEA in line with the allocation.

## A. Data Map

The data map should outline the flow of data between the participants, relevant parties, processors, and systems.



## B. Describe the purpose of the processing

The **purpose of the processing** is the reason why you want to process the personal data.

Question	Answer
What do you want to achieve?	Financial support in respect of Irish students with disabilities at UK/EEA HEIs
What are the benefits of the processing for you, and more broadly?	The processing is necessary to enable administration of the fund and provision of the relevant funding to the HEIs. It would not be possible to allocate funding without the data.
If there an expected/intended effect on individuals?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Comments: There should be no effect on individual students other than received financial support.

## C. Describe the nature of the processing

The **nature** of the processing is what you plan to do with the personal data.

Question	Answer
What categories of personal data is being used?	<input checked="" type="checkbox"/> Personal <input checked="" type="checkbox"/> Special Category <input type="checkbox"/> Criminal
What types of data will be used in the process? e.g. contact details, demographics, location.	Student name, Course, Disability, Specialist reports, Supports to be provided to the student
How will you collect and use the data?	Through the return of application forms and annual reports.
How will you store and delete the data?	The data is stored on the HEA Access drive and is subject to the HEA's data retention policy.
What is the source(s) of the data?	The participating students and HEIs are the source of the data.

## D. Describe the scope of the processing

The **scope** of the processing is what the processing covers.

Question	Answer
What number of data subjects will be involved in the processing?	Applications are received for approximately 250 individuals.

What is the geographical extent of the processing? (e.g. town, county, province)	The fund is open Irish citizens studying in HEIs in the EEA/UK. In recent years, only applications from students registered in the UK have been received by the HEA.
What is the volume of data and/or range of different data items being processed?	The number of applications would typically be around 200-250 each year. Along with general details such student's demographic details, information about the course, student's disabilities, and supports to be provided to the student, together with the relevant specialist reports.
What is the expected duration of the processing activity?	Approximately 6 months annually.
How long will you retain the data for?	For no longer than necessary, for the duration of the processing.  FSD data retained is subject to the HEA's data retention policy.

## E. Describe the context of the processing

The **context** of the processing is the wider picture, including internal and external factors which might affect expectations or impact.

Question	Answer
Do the processing include children or other vulnerable groups of data subjects?	<input type="checkbox"/> Patients <input type="checkbox"/> Elderly <input type="checkbox"/> Children <input type="checkbox"/> Other Students with disabilities are included in the processing.
What is the nature of your relationship with the individuals?	The HEA do not have any direct relationship with the individuals.
Could refusing participation impact the individuals use of a service or application of their rights?	Yes. If a student does not provide their personal details, the institution cannot receive funding under the FSD in respect of such student's needs. However, institutions can provide supports outside of the scope of FSD.
Are there any current issues of public concern that you should factor in? e.g. monitoring of publicly accessible areas	Not that we are aware of.

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?	Not that we are aware of
--	--------------------------

### F. Consultation Process

The consultation process should aim to incorporate the views of data subjects (where appropriate), internal stakeholders (including DPO within your organisation), external stakeholders and independent experts.

Question	Answer						
Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.	FSD has been established many years ago, together with the relevant processes. The HEA administers the fund on behalf of DFHERIS.						
Who else do you need to involve within your organisation?	The HEA DPO and Access Policy section.						
Do you plan to consult information security experts, or any other experts?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Comments: IT Security experts						
Are there any other data controllers involved in this processing relationship?	<input checked="" type="checkbox"/> Controllers <input type="checkbox"/> Joint Controllers Comments:						
Do you need to engage with these controllers?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Comments: They are responsible for returning the data to the HEA as part of the students funding application.						
Are there any data processors involved in this processing relationship?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Comments:						
Do you need to engage with these processors?	<input type="checkbox"/> Yes <input type="checkbox"/> No Comments: N/A						
What measures do you take to ensure processors comply?	<table border="1"> <tr> <td>Data Processing Agreement</td> <td>Vendor Assurance Assessment</td> </tr> <tr> <td><input type="checkbox"/> Yes</td> <td><input type="checkbox"/> Yes</td> </tr> <tr> <td><input type="checkbox"/> No</td> <td><input type="checkbox"/> No</td> </tr> </table>	Data Processing Agreement	Vendor Assurance Assessment	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> No
	Data Processing Agreement	Vendor Assurance Assessment					
<input type="checkbox"/> Yes	<input type="checkbox"/> Yes						
<input type="checkbox"/> No	<input type="checkbox"/> No						



## G. Necessity & Proportionality

When assessing the necessity & proportionality of the processing, consider the following:

- **Necessity** states that the limiting of the fundamental right to the protection of personal data must be strictly necessary.
- **Proportionality** requires a balance between the means used and the intended aim. The limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure.

Question	Answer
What is your lawful basis for processing?	<input type="checkbox"/> Consent <input type="checkbox"/> Contract <input type="checkbox"/> Legal obligation <input type="checkbox"/> Vital interests <input checked="" type="checkbox"/> Public task <input type="checkbox"/> Legitimate interests
If applicable, what is your lawful basis for processing special categories of data?	<input type="checkbox"/> Consent <input type="checkbox"/> Employment <input type="checkbox"/> Vital interests <input type="checkbox"/> Legitimate interests by foundation, association of non-profit <input type="checkbox"/> Publicly available information <input type="checkbox"/> Legal claims <input checked="" type="checkbox"/> Public interest <input type="checkbox"/> Healthcare <input type="checkbox"/> Public interest regarding public health <input type="checkbox"/> Archiving, research, or statistical purposes in public interest
Is there any other legislation which supports this processing? e.g. Data Protection Act 2018, Statutory instruments, or other regulations.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <div style="margin-left: 150px;">Comments: Data Protection Act 2018</div>
Does the processing achieve your purpose?	Yes, it allows the HEA fulfil its funding obligations.
Is there another way to achieve the same outcome?	No.
How will you prevent data being used for a different purpose than for which it was collected? i.e. function creep	The HEA do not use the data for any purpose other than to satisfy HEA obligations. Internal policies and procedures are in place to prevent use of the data for other purposes.

	<p>Files with UK/EEA student data are stored on the HEA's shared drive and only those staff members who are involved in administration of the Fund have access to them. The collated UK/EEA data files used to allocate funds are accessible only to the Senior manager and staff members involved in the administration of the Fund.</p> <p>The senior manager responsible for overseeing the UK/EEA collection process is aware of the sensitivity of the data and data protection requirements. The relevant staff members are also aware of these requirements and cognisant that it is not permissible to use data for other purposes.</p> <p>New staff receive HEA induction which includes the area of data protection. The relevant standard operational procedure includes a data protection related section.</p>
<p>How will you prevent data linkages or unintended matching of data sets?</p>	<p>As the students are enrolled in higher education institutions outside of Ireland, the HEA does not collect information pertaining to these students as a part of HEA's remit and normal data processing activities. Therefore, it is highly unlikely that data linkages or unintended matching of data sets could occur.</p> <p>Other staff members of the HEA do not have access to the data.</p>
<p>How will you ensure data quality and accuracy?</p>	<p>The HEA receives the data from HEIs which are responsible for data quality and accuracy. Guidelines for completing the return are provided to HEIs to ensure consistency in approach to return within the sector.</p> <p>The HEA carry out checks of returns received and liaises with institutions where issues are identified. A standard operational procedure is in place for processing of UK/EEA returns.</p>
<p>Are measures in place to ensure the collection of unnecessary data is minimised?</p>	<p>A review of the application form and returns is undertaken on annual basis as a part of updating of the annual FSD UK/EEA Guidelines.</p>

	<p>The modalities of the Fund and relevant reporting requirements are considered to ensure that only necessary data is collected.</p> <p>Only questions and supporting documentation needed to establish the students' eligibility for funding and the appropriateness of supports/costings are requested.</p>
Which of the rights are you able to support?	<input type="checkbox"/> Erasure <input checked="" type="checkbox"/> Portability <input checked="" type="checkbox"/> Access <input checked="" type="checkbox"/> Restriction <input type="checkbox"/> Objection <input type="checkbox"/> Rectification
If you cannot support any rights, outline why.	Erasure and Objection cannot be supported because funding cannot be allocated to institutions without the relevant data. Aggregated data is used for future fund allocation modelling, statistical, and policy purposes.
Will you be transferring personal data internationally?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <p>Country: UK or an EEA country, in which is the relevant HEI (which submits the application for funding) located, as queries are being clarified with the concerned HEI and notification of amounts allocated is provided to the concerned HEI.</p>
If applicable, how will you safeguard the international transfer of personal data?	<input checked="" type="checkbox"/> Adequacy agreement <input type="checkbox"/> Standard contractual clauses <input type="checkbox"/> Binding corporate rules <input type="checkbox"/> Approved code of conduct <input type="checkbox"/> Approved certification mechanism <input type="checkbox"/> Approved ad-hoc contracts <input type="checkbox"/> Derogation

## H. Security

Question	Answer
Are there prior concerns over this type of processing or security flaws?	The data is being submitted to the HEA by email which has certain risks associated. To reduce the risk, use of password protection is encouraged. As the HEA will be implementing new organization-wide IT

	systems such as a Customer Relationships Management solution, a possibility of alternative means for FSD UK/EEA submissions and associated data transfers will be explored.
What is the current state of technology in this area?	The HEA will explore the possibility of implementing a portal to support FSD operation, within its new CRM or grant management solution.
Is there new technology being used or new processing being conducted as part of the project? e.g. new software to analyse data or new methods of data collection etc.	No
Are safeguards in place to limit access to personal data? Provide summary of safeguards.	Yes, technical, and organisational measures are in place: Files are stored on HEA's shared drive and only authorised staff has access to the relevant folders. HEA staff receives data protection training.
Are safeguards in place to limit unauthorised processing of personal data? Provide summary of safeguards.	Yes, technical, and organisational measures are in place. HEA staff receives data protection training.
Are security measures in place to protect the data? Provide summary of safeguards.	Files are stored on HEA's shared drive and only authorised staff has access to the relevant folders. A system of regular backups supported by HEA IT department is in place.

### 3. IDENTIFY & ASSESS RISKS

**Describe the source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary.

To effectively assess risks, the information provided in the previous sections should be reviewed and assessed against the principles of data protection (see Appendix A) and universal privacy risks (Appendix B). Appendix C provides guidance on assessing risks.

If any of the risks outlined cannot be managed and the **residual risk remains high**, the Data Protection Commissioner must be contacted before moving forward with the project, this is a requirement under GDPR.

Risk No.	1. Lawful, Fair & Transparent: Personal data is processed lawfully, fairly and in a transparent manner.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
1.1	HEA legislation is old and outdated (HEA Act 1971), the legal basis is not considered sufficient.	Reasonable	Minimal	Low	HEA legislation is being updated.	Low
1.2		Reasonable	Some	Medium		Medium
1.3		Reasonable	Serious	High		High

Risk No.	<b>2. Purpose limitation:</b> Personal data is only collected for pre-specified, explicit, and legitimate purposes and not for further processed if this is incompatible with those purposes.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
2.1	That the student's data will be further processed by the HEA for funding models.	Remote	Some	Low	The HEA only use the data for its intended purposes of funding Irish students in UK/EEA HEIs and reporting. It is not further processed by the HEA.  HEA collects data needed for funding models separately.	Low
2.2						
2.3						
Risk No.	<b>3. Data minimisation:</b> Personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
3.1	That student data that is not required for agreed reporting purposes will be forwarded by the HEI for processing by the HEA.	Remote	Some	Low	Only data that is required by the HEA for funding purposes is collected and processed. If data irrelevant to the purposes for which it is collected is received, it will be destroyed and the relevant HEI advised.	Low
3.2						
3.3						

Risk No.	4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
4.1	That inaccurate or incorrect data on the data subject will be collected and stored by the HEA.	Remote	Some	Low	The HEIs are collecting the data while engaging directly with the relevant students and the data is self-declared. Students are signing the application and declaring that the data is accurate.	Low
4.2						
4.3						
Risk No.	5. Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
5.1	That the student's personal data will be kept for longer than required under current HEA requirements.	Remote	Some	Low	The data will not be kept beyond the point where it is no longer required. The Third Level Access annual workplan incorporates a review of records to ensure adherence to the HEA's record retention policy.	Low
5.2						
5.3						

Risk No.	<b>6. Security, Integrity and Confidentiality:</b> Personal data shall be processed in a manner that ensures appropriate security of the personal data.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
6.1	That the data subject's information might be shared or processed by persons who do not have the correct authority to do so within the HEA.	Reasonable	Some	Medium	Technical and organisational measures are implemented to safeguard against any improper sharing or processing of data within the HEA. Data is not shared outside of the HEA.	Medium
6.2						
6.3						
Risk No.	<b>7. Accountability:</b> It should be demonstrable that personal data is processed in line with data protection principles.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
7.1	That student's personal data will be processed in a manner that is not on keeping with data protection principles.	Remote	Some	Medium	Staff will undertake regular training and refreshing of principles of data protection. Technical and organisational measures are periodically reviewed.	Low
7.2						
7.3						



Risk No.	<b>8. Rights of Individuals:</b> Data subjects have the right to request for access, rectification, portability, or erasure of their personal data or to object to the processing method.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
8.1	That data subjects will not be able to exercise their rights over their data.	Remote	Some	Low	Data subjects who benefit from the FSD programme may not have right to have their data erased. However, they may request access, rectification etc.	Low
8.2						
8.3						
Risk No.	<b>9. Transfers to Third Countries:</b> Personal data shall only be passed on to a country outside the European Economic Area (EEA) if that country ensures an adequate level of privacy protection.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
9.1	That data subject's personal information will be shared and processed outside of the EU/EEA,	Remote	Some	Low	Organizational measures are in place to prevent that data are transferred outside of the EU/EEA.	Low
9.2						
9.3						

Risk No.	10. Other risks.	Likelihood	Severity	Risk Level	Mitigating Action	Residual Risk
10.1						
10.2						
10.3						

## 4. RISK MITIGATION

As outlined in the table above.

## 5. APPROVAL & SIGN OFF

### Approval considerations (e.g. DPO or external consultant advice)

Comments:

### Data Protection Officer

Signed: ...Éilis Noonan.....

Date: .....5 April 2022.....

### Business Owner

Signed: .....

Date: .....

# APPENDIX A – PRINCIPLES OF DATA PROTECTION

The starting point of a DPIA is to identify the relevant privacy principles. Based on research from different sources, several privacy principles are identified, which are relevant to an assessment of the design of a new system or change in existing processing of personal data or another use of existing systems and related data processing.

1. **Lawfulness, fairness, and transparency:** Personal data shall be processed lawfully, fairly and in a transparent manner.
  - Has a lawful basis for the processing activity been identified?
  - Is the processing listed in the Record of Processing Activities?
  - Does the processing seem fair, i.e. not excessive?
  - Are we being transparent about the processing? Has the type of processing been identified in the privacy notice or has the data subject been otherwise informed?
2. **Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes.
  - Will this new project/processing activity involve data being processed in a manner for which it was not collected?
  - Have we been transparent about any extra processes? Is the processing still lawful?
3. **Data minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
  - Are we excessively collecting or processing data?
  - Is the system processing data for purposes other than the purpose for which it was established?
  - Is the data being processed relevant to the purpose?
4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay?
  - Are there measures which guarantee the accuracy and correctness of the personal data processed within the information system?
  - Can data be updated, where required?
  - How often is data updated? Is this frequently enough?
5. **Storage Limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
  - Does the system allow data to be deleted when it is no longer required?
  - What retention periods are being implemented? Has a clear justification for these retention periods been established?
  - If data is anonymised/pseudo-anonymised, are we sure that a person cannot be identified using the retained data?

6. **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
  - Have appropriate security controls been implemented to protect the data?
  - Has the IT team been consulted on the effectiveness of the controls in place? Are they in line with ISO27001 or another information security standard?
  - Are the controls which have been implemented proportionate to the nature of the data?
7. **Accountability:** The responsible entities also known as “controllers” take measures to implement programs to eliminate or mitigate privacy risks on strategic, tactical, and operational level. Assurance of these measures includes the proof of monitoring of these risks, internal and/or external audit and potentially reporting to external stakeholders like privacy authorities or data protection regulators.
  - Are any risks identified being monitored effectively?
  - Can any decisions made be justified and are documented should an audit take place?
8. **Rights of Individuals:** Citizens and consumers have the right request for access, rectification, portability, or erasure of their personal data or to oppose the processing method. The individual may ask which authorities have been provided with personal data and which authorities have received their personal data.
  - Does the system impose restrictions on the ability to comply with valid subject right requests?
9. **Transfers to Third Countries:** Personal data shall only be passed on to a country outside the European Union (EU) and European Economic Area (EEA) if that country ensures an adequate level of privacy protection.
  - Have appropriate safeguards been established for any transfers of data outside the EU/EEA? (e.g. adequacy agreement or standard contractual clauses)

## APPENDIX B –PRIVACY RISKS

There are a range of different ways that an individual's data privacy can be compromised or put at risk by a new project. The types of risk range from the risk of causing distress, upset or inconvenience to risks of financial loss or physical harm. There are equally as many kinds of data privacy-related risks to organisations, related to compliance issues and commercial factors.

Look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- reidentification of pseudonymised data;
- or any other significant economic or social disadvantage.

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

### Example of Risks to Individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- 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.

### Examples of Corporate Risks

- Non-compliance with 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.
- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.
- Data losses which damage individuals could lead to claims for compensation.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.

## Examples of Compliance Risks

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the Data Protection Acts 1988 & 2003/ General Data Protection Regulation (GDPR).
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR)/e-Privacy Regulation.
- Non-compliance with sector specific legislation or standards e.g. Health Information and Quality Authority (HIQA), Health and Safety Authority (HSA).
- Non-compliance with human rights legislation United Nations Declaration on human Rights (UNDHR).



## APPENDIX C – ASSESSING RISK

Consider the potential impact on individuals and any harm or damage your processing may cause – whether physical, emotional, or material. In particular, look at whether the processing could contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, you need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm may still count as high risk.

You must make an objective assessment of the risks. It is helpful to use a structured matrix to think about likelihood and severity of risks:

<b>Severity of impact</b>	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		<b>Likelihood of harm</b>		

