DATA PROTECTION IMPACT ASSESSMENT REPORT

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

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:	The primary objective of the data processing is to assist with the modelling of the 'Fund for Students with Disabilities' (FSD) allocations for Irish HEIs participating in the Fund. Aggregated data is used to inform recurrent grant allocation (RGAM) to HEA designated institutions. Aggregated data is used for statistical and policy purposes.
Summary of processing:	Required personal and special category data for the purposes of determining FSD allocations is requested and gathered on data subjects from the Higher Education Institutions (HEIs). The HEA issues a excel template file to HEIs i.e., 'Resource Allocation Return' (RAR). HEIs use this template to gather the data during the academic year. HEIs forward their completed return to the HEA at the end of the academic year and the HEA solely uses the data collected to model FSD allocations for HEIs for the next calendar year. The collated file is then anonymised and saved on the drive and may be used for non-personalised reporting of data on FSD.
Why have you identified the need for a DPIA? Refer to risk assessment findings.	The HEA are responsible for processing sensitive personal student data, including Special Category Data.
Identify any associated documentation which is relevant to this DPIA.	- Data Sharing Agreements with participating HEIs - Annual FSD guidelines to Irish HEIs - Internal standard operational procedures pertaining to administration of FSD (Allocations Modelling, RAR Verifications)

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.**

The purpose of the processing is to enable modelling of FSD allocations to HEIs. The allocation model was put in place based on recommendations of a review of the fund, starting from 2019, and is based on categories and extent of support provided to students. Therefore personal and special category data are necessary for the purposes of modelling allocations. The FSD fund helps to support the equality of access for students with disabilities in third level education.

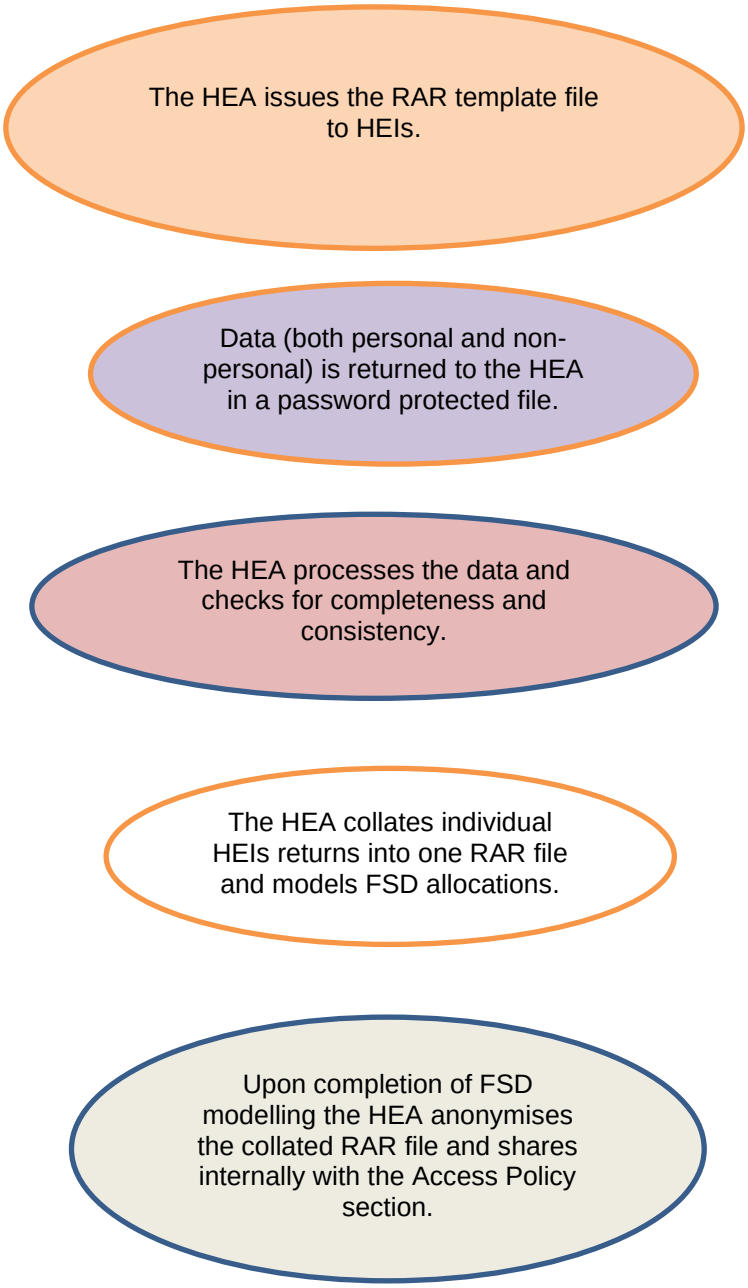
Systems Funding staff members who prepare FSD allocations process the personal data collected.

The HEA issues a 'Resource Allocation Return' template to HEIs at the beginning of the academic year requesting HEIs to complete during the academic year. Data collected include student reference number, information about student's disability/s, details of supports that were provided and costs incurred by the HEIs during the academic year. Information such as level of the course attended, mode of study full time/part time is required for statistical and policy purposes.

The spreadsheets are structured and specific tools such as drop-down lists and formulae are implemented to ensure that the information is complete and consistent, meeting the applicable standards. Once completed, HEIs password protect their completed file and submits the return to the HEA. The HEA checks and verifies the data for completeness and consistency, following an internal standard operational procedure. The individual RARs are then collated into one file and allocations are modelled.

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?	To allocate FSD funding in line with the applicable funding model.	
What are the benefits of the processing for you, and more broadly?	The processing is necessary for allocating funding according to the funding model. It would not be possible to allocate funding without the data.	
If there an expected/intended effect on individuals?	☐ Yes ☐ No	Comments: There should be no effect on individual students.

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?	☐ Personal ☐ Special Category ☐ Criminal
What types of data will be used in the process? e.g. contact details, demographics, location.	Student reference number, Course, Disability, Supports provided to the student
How will you collect and use the data?	The data is collected through password protected spreadsheet file.
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 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?	The number of students supported by FSD varies across each HEI depending on their size. In total c. 15,000 students are supported annually under the fund. As the student population increases the number of students expected to benefit from the fund also increases.
What is the geographical extent of the processing? (e.g. town, county, province)	Information is only sought from data subjects studying at Irish HEIs participating in the programme, they will be located throughout the country. Non-Irish nationals may also be included as we have no way of knowing their nationality (EU students and students from the EEA, Switzerland and the UK are eligible for supports). The HEA are not able to identify the location of any of the data subjects.
What is the volume of data and/or range of different data items being processed?	The data subject's reference number, course information, disability information, supports received and cost associated. In general, one row in the return corresponds to one data subject. See Appendix D below.
What is the expected duration of the processing activity?	Approximately 6 months (October to March) 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?	☐ Patients ☐ Elderly ☐ Children ☐ Other	Students with disabilities are included in the processing.
What is the nature of your relationship with the individuals?	Currently the HEA do not have any direct relationship with the data subjects.	

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. The HEA engages with HEIs as the fund in being administered, and HEA also engages with the DAWN group which represents the sector in the FSD Implementation Group.	
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?	☐ Yes ☐ No	Comments: IT security experts
Are there any other data controllers involved in this processing relationship?	☐ Controllers ☐ Joint Controllers	Comments:
Do you need to engage with these controllers?	☐ Yes ☐ No	Comments:
Are there any data processors involved in this processing relationship?	☐ Yes ☐ No	Comments:
Do you need to engage with these processors?	☐ Yes ☐ No	Comments: N/A

What measures do you take to ensure processors comply?	Data Processing Agreement ☐ Yes ☐ No	Vendor Assurance Assessment ☐ Yes ☐ 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?	☐ Consent ☐ Contract ☐ Legal obligation ☐ Vital interests ☐ Public task ☐ Legitimate interests	
If applicable, what is your lawful basis for processing special categories of data?	☐ Consent ☐ Employment ☐ Vital interests ☐ Legitimate interests by foundation, association of non-profit ☐ Publicly available information ☐ Legal claims ☐ Public interest ☐ Healthcare ☐ Public interest regarding public health ☐ 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.	☐ Yes ☐ No	Comments: Data Protection Act 2018

Does the processing achieve your purpose?	Yes.
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	Files with FSD 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 RAR file used to model allocations is password protected and only the Senior manager and staff members involved in FSD personal data processing are aware of the password. The senior manager responsible for overseeing the RAR 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. New staff receive HEA induction which includes the area of data protection. The relevant standard operational procedure includes a data protection related section.
How will you prevent data linkages or unintended matching of data sets?	HEIs are advised to use an FSD specific student identifier, which will not allow to identify data subjects outside of the institution i.e. by the HEA or in case of a data breach by any other party. HEIs are also specifically advised not to use PPS number for the purposes of FSD related returns. The relevant staff members who process this data are aware that this is not permissible. Other HEA staff members do not have access to FSD data as access is restricted to the relevant staff only.
How will you ensure data quality and accuracy?	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.

	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 RAR returns.
Are measures in place to ensure the collection of unnecessary data is minimised?	A review of the structure of the RAR return was undertaken as a part of implementation of the revised FSD allocation model in 2019. Several categories of data previously included in the template were identified in consultation with HEA Access Policy section as unnecessary for the specified purpose, removed from the template and their collection was discontinued. The template is reviewed on annual basis at the time when FSD Guidelines for the new academic year are being prepared. The modalities of the Fund and relevant reporting requirements are considered to ensure that only necessary data is collected.
Which of the rights are you able to support?	☐ Erasure ☐ Portability ☐ Access ☐ Restriction ☐ Objection ☐ 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. Anonymized returns are retained for statistical and policy purposes. Aggregated data is used to inform recurrent grant allocation to institutions.
Will you be transferring personal data internationally?	☐ Yes ☐ No Country:
If applicable, how will you safeguard the international transfer of personal data?	☐ Adequacy agreement ☐ Standard contractual clauses ☐ Binding corporate rules ☐ Approved code of conduct ☐ Approved certification mechanism ☐ Approved ad-hoc contracts ☐ Derogation

H. Security

Question	Answer

Are there prior concerns over this type of processing or security flaws?	Previously FSD related returns with personal data were sent to the HEA by email. To reduce the risk to security of the data, HEIs are now requested to submit returns using the HEAnet FileSend facility and use passwords agreed individually between each institution and the HEA.
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: Once the personal data has been processed for FSD modelling of allocations, the collated RAR file is anonymised. 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	Information about data processing is not sufficiently transparent from the data subject's point of view.	Reasonable	Some	Medium	HEA reviews the relevant documentation on annual basis as FSD Guidelines are updated for the new academic year. Feedback received from the HEIs and other stakeholders is considered.	Low
Risk No.	**2. Purpose limitation:** 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.	Remote	Some	Low	The HEA do not use the data except for the purpose for which it is collected by the HEIs and returned to the HEA. Internal technical and operational measures are in	Low

					place to prevent further processing incompatible with the purposes for which the data is being collected. The specific mitigating measures in place are: • Anonymising the FSD modelling file when the process of modelling FSD allocations is completed, deleting individual returns received from institutions • Access to data on the shared drive granted to authorised HEA staff members only • Adherence to the HEA's data retention policy • Adherence to Internal IT security policy	
Risk No.	**3. Data minimisation:** 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 FSD modelling purposes will be forwarded to the HEA for processing.	Remote	Some	Low	A review of the template is undertaken on annual basis to ensure that only necessary data is collected. RAR returns are checked upon receipt and if additional data is identified, the relevant HEI will be notified and the additional data deleted.	Low
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.	Reasonable	Low	Low	Thorough checks are undertaken by the HEA staff to ensure that the data provided is complete and consistent in order to mitigate this risk. Where issues are identified, clarifications / corrections are requested from the HEIs.	Low

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	Remote	Some	Low	HEA encourages HEIs to use an FSD specific identifier, so that students cannot be identified within the HEA. HEIs are advised not to use PPS numbers and institutional student IDs in FSD returns. Identifying data are being removed by the HEA once modelling of allocations is completed. Mitigating actions • Adherence to the HEA's data retention policy	Low
Risk No.	**6. Security, Integrity and Confidentiality:** 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 either within the HEA or the HEI who collect it.	Reasonable	Some	Medium	Controls are implemented to safeguard against any improper sharing or processing of data within the HEA. Only authorised HEA staff members have access to the data and they are aware of the data protection implications, in line with the standard operational procedures in places. When liaising with the relevant HEIs where data need to be exchanged, files with the data will be password	Low

					protected using a password agreed separately with each individual HEI. Internal IT security policy is also in place as a mitigating measure against this risk.	
Risk No.	**7. Accountability:** 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 information available to external stakeholders about FSD and the relevant data processing is not sufficient.	Reasonable	Some	Medium	FSD Guidelines are circulated on annual basis, HEA engages with the sector via the DAWN group. The DPIA report and a data collection notice will be made available on the HEA website.	Low
Risk No.	**8. Rights of Individuals:** 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	The HEA might not be able to support the right to erasure and the right to object. Other data subjects' rights will be supported. The HEA will be transparent about the above limitations to data subjects' rights.	Low
Risk No.	**9. Transfers to Third Countries:** 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	The data is not intended to be provided to subjects outside of the EEA.	Remote	Some	Low	All staff who has access to FSD data is aware of the applicable restrictions in place.	Low

					Access to data is restricted to authorised HEA staff members only. Password protection is applied on files that are being sent between the HEA and the HEIs.	
Risk No.	**10. Other risks.**	**Likelihood**	**Severity**	**Risk Level**	**Mitigating Action**	**Residual Risk**
10.1	No FSD specific other risks have been identified.					

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: …Andrea Valova……..	Date: …6 October 2021……

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:

Severity of impact				
	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
		Likelihood of harm		

APPENDIX D – RAR RETURN SPREADSHEET

Blank RAR Return.xlsx