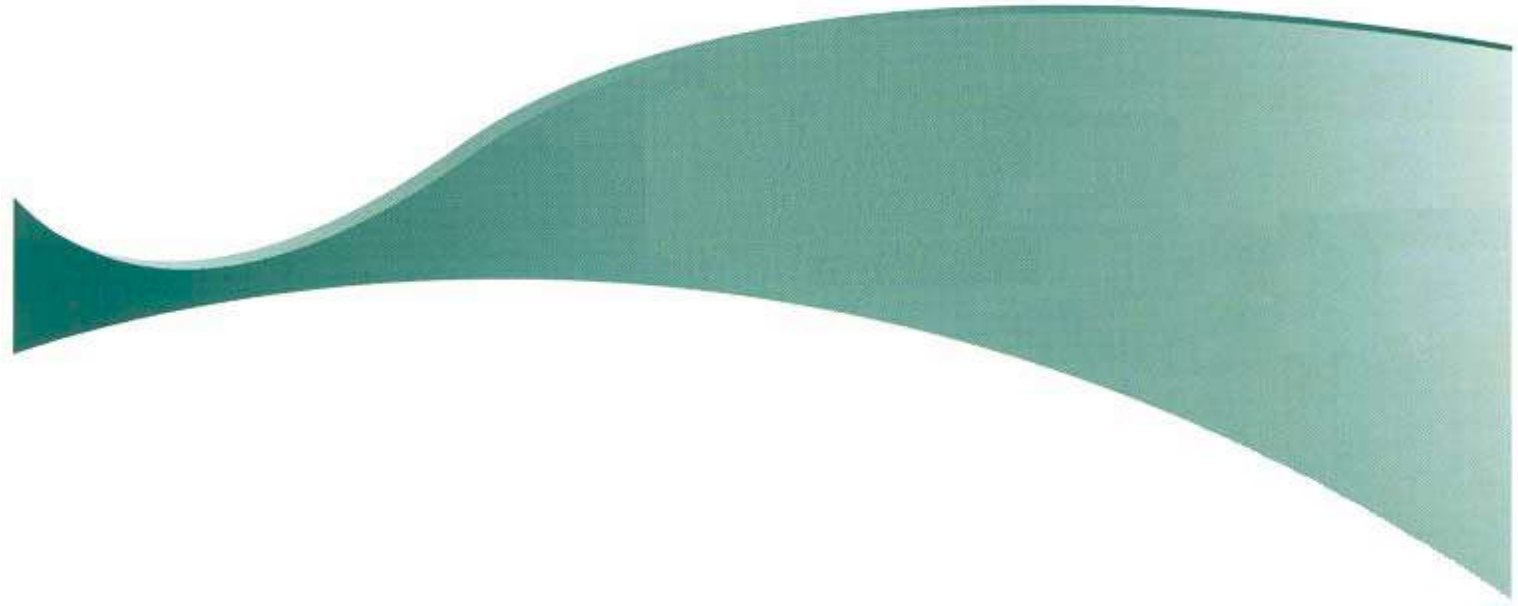
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

HSE Privacy Impact Assessment (PIA) Process Guidance



This Guidance document should be read in conjunction with the HSE Privacy Impact Assessment Form

June 2019

What is a Privacy Impact Assessment (PIA)?

Under Article 35 of the General Data Protection Regulation (GDPR) there is an obligation to do a Privacy Impact Assessment before carrying out types of processing likely to result in high risk to the rights and freedoms of individuals. A PIA is a process to help identify and minimise the data privacy risks of a project or activity so as to ensure that patients and service users' rights to privacy and confidentiality are appropriately protected. The PIA is an important element of the key GDPR themes of accountability and data protection by design. The DPO/DDPO can be contacted for advice at the initial stages of the PIA programme and on-going as required.

A **Data Controller** is a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.

A **Data Processor** is a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.

Section 1 – Initial details (Threshold Assessment)

The PIA needs to be included in the design phase of the project or activity where personal data is going to be processed. The project lead should take ownership of ensuring that this piece of work has been appropriately carried out. **Personal data** is any information relating to an identified or identifiable natural person (Data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

A PIA is needed when there is a likely risk to the rights and freedoms of data subjects. This would include when new data processing technology is being used or when a new process is being used. A PIA is needed for the large scale processing of special categories of data, for the systematic monitoring of publically accessible space or for profiling operations.

It is the controller that has to decide if the PIA is needed and ultimately has to sign-off on the processing after the PIA is completed.

If no PIA is needed, the controller can give approval for the processing to begin, however it must be documented that careful consideration has been given as to whether or not a PIA was required and the relevant factors examined to come to the conclusion that one is not required in this particular case.

If the controller decides a PIA is needed, the project lead will have to start the PIA. The PIA should be undertaken by individuals who have the appropriate expertise and knowledge of the

project in question and who have undergone the HSELanD GDPR/Data Protection Awareness Training.

Section 2 – Activity Details

Characterise Processing Operation

It is important to identify how the data will be collected, used, stored and deleted in the project. You will need to identify what kind of information will be used and who will have access to it. You may need to consult with the various stakeholders to identify the technical aspects of how the data will be collected, stored and processed during the project. It is also important to consider if more personal data will be created as a result of the processing and how this data will be stored, used and deleted. The retention period for the data also needs to be considered. You will need to identify the legal basis for processing and document it. For health related data and other special categories of personal data, you will also need to identify a legal basis for processing the special categories of data. More details on the legal bases for processing can be found in the HSE data protection policy here.

Automated decision making is a decision or decisions made solely by automated means i.e. without any human involvement. Data subjects have the right to object to automated decision making and it is only allowed in certain circumstances.

European Economic Area (EEA) is the area in which the agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area. The list of EEA countries are in the table below.

Austria	Belgium	Bulgaria	Croatia
Cyprus	Czech Republic	Denmark	Estonia
Finland	France	Germany	Greece
Hungary	Iceland	Ireland	Italy
Latvia	Liechtenstein	Lithuania	Luxembourg
Malta	Netherlands	Norway	Poland
Portugal	Romania	Slovakia	Slovenia
Spain	Sweden	Switzerland	United Kingdom*

*The status of the United Kingdom needs to be confirmed prior to completing a PIA.

In general a **transfer of personal data** to a country outside of the EEA is only allowed where the controller and processor are compliant with the GDPR. To legally transfer data to countries outside of the EEA you must have:

1. Acquired and processed the data legally and be attempting to transfer the data in line with the original reason for collecting the data (i.e. For the purposes of occupational medicine)
2. A legal basis for the transfer. The legal bases should be considered in the following order:

a. Adequacy Decision – An adequacy decision is when the EU commission comes to the decision that country in question has adequate data protection (equivalent to GDPR) so as to allow transfer (currently allowed countries are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US)

b. Appropriate Safeguards – For example, a legally binding contract, use of standard data protection clauses provided by the EU Commission etc.

c. Specific Derogation - Transfers are allowed where the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent. This is only permitted in once-off situations

Organisational Security Measures might include policies, procedures, training and audit trails. The following are some examples:

- communicating to employees the importance of company data and the measures they can take to protect it;
- conducting on-going staff training on, but not limited to, social engineering attacks, crypto ransomware, and data protection;
- documenting data collection and retention policies;
- ensuring the use of strong passwords by having a password policy in place that is enforced;
- ensuring remote access is supported by a remote access policy;
- documenting a data breach incident response plan and testing it periodically to ensure a data breach can be effectively responded to;
- documenting CCTV policies (where appropriate);
- documenting data back-up policies;
- periodically reviewing contracts with 3rd party ICT providers to ensure the security measures documented are still appropriate and up to date.

Technical Security Measures refer to the technical controls in place to protect personal data the following are some examples:

- ensuring that all computing devices such as PCs, mobile phones, and tablets are using an up-to-date operating system;
- ensuring all computing devices are regularly updated with manufacturer's software and security patches;
- using antivirus software on all devices;
- implementing a strong firewall;
- reviewing vendor supplied software and updating default system, administrator, and root passwords and other security parameters to ensure defaults are not left in place;
- ensuring data backups are taken and are stored securely in a separate location;
- ensuring that data backups are periodically reviewed and tested to ensure they are functioning correctly;
- ensuring that data is collected & stored securely;
- ensuring that mobile devices (such as laptops and mobile phones and tablets) are encrypted;

- ensuring that two-factor authentication is enabled for remote access;
- ensuring that websites have TLS (transport layer security) in place to securely collect personal data via webforms (such as for newsletter subscriptions) or on ecommerce websites.

Section 3 – Research

Confirmation that the *Data Protection Act 2018 (Section 36(2))(Health Research) Regulations 2018* has been applied to this PIA where relevant.

Under the above named Regulations (and any subsequent amendments) researchers must ensure that suitable and specific measures are taken to safeguard the fundamental rights and freedoms of the data subjects involved in the research. Therefore for a researcher who is completing the PIA It will be necessary to complete this section in order to confirm compliance with these research Regulations,

Section 4 – Risks and Risk Mitigation

Identify Risks

Identify the risks that are likely to be posed to the data subject and the risks posed to the HSE. The risks to data subjects may include non-data protection rights and freedoms – risk in this context is about the potential for any significant physical, material or non-material harm to individuals which include the risk of causing distress or financial loss. Risks to the HSE include the risk of breaching GDPR or incurring data breaches which could result in financial penalties.

As per Article 29 working party guidelines, the risk will be grouped into the categories below:

Is there a risk of:	a. ☐ Illegitimate access to personal data b. ☐ Unwanted modification to personal data c. ☐ Personal data disappearance d. ☐ Other (please state)

To identify the risks, it is helpful to consider what the reason for conducting the PIA in the first place was.

The DPC has outlined the following potential risks:

a. *Illegitimate access to personal data*
   - The data is seen by an unauthorised person
   - The data is copied and saved to another location
   - The data is disseminated more than necessary and beyond the control of the data subject

- The data is used for purposes other than those planned and/or in an unfair manner
- Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- Breach of data held electronically by “hackers”.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Data may be kept longer than required in the absence of appropriate policies.
- Accidental loss of electronic equipment by personnel may lead to risk of disclosure of personal information to third parties.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Data may be transferred to countries with inadequate data protection regimes.

b. *Unwanted modification to personal data*
    - The data is modified into valid or invalid data, which will not be used correctly, the processing is liable to cause errors, malfunctions, or no longer provide the expected service
    - The data is modified in such a way that the processing operations have been or could be misused

c. *Personal data disappearance*
    - The data is missing for personal data processing, which generates errors, malfunctions, or provides a different service than the one expected (e.g. some allergies are no longer reported in a medical record or the inability to provide care due to the loss of medical records)

d. *Other*
    - Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
    - Personal data being used for automated decision making may be seen as excessively intrusive.
    - Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
    - Collection of data containing identifiers may prevent users from using a service anonymously.
    - Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.

Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions

Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.

Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation.

Rating the potential risk using the Privacy risk matrix:

A risk matrix is a useful tool for ranking and displaying risks by defining ranges for the likelihood and impact of risks occurring. The risk is a combination of the likelihood and impact of the risk occurring.

Likelihood	Score	Description
Rare	1	Possible to occur but no known precedents
Unlikely	2	Has occurred infrequently in the past, or, a “one off” from the past
Possible	3	Has occurred a few times in the past, or, has occurred infrequently in recent history
Likely	4	Has occurred many times in the past, or has occurred a few times in recent history
Highly likely	5	Is a feature of projects of this type, or has occurred many times in recent history, or is a brand new risk that has been identified that is imminent

Impact	Score	Description
Negligible	1	Negligible impact on data subjects
Minor	2	Minor impact on a small number of data subjects
Moderate	3	Moderate impact on data subjects or a low impact on a large number of data subjects
Major	4	Major impact on data subjects or a medium impact on a large number of data subjects
Critical	5	Critical impact on data subjects or a high impact on a large number of data subjects

	Likelihood				
Impact	Rare 1	Unlikely 2	Possible 3	Likely 4	Highly likely 5
Negligible – 1	**1**	**2**	**3**	**4**	**5**
Minor – 2	**2**	**4**	**6**	**8**	**10**
Moderate – 3	**3**	**6**	**9**	**12**	**15**
Major – 4	**4**	**8**	**12**	**16**	**20**
Critical – 5	**5**	**10**	**15**	**20**	**25**

Low (1 – 7) **Medium (8-14)** **High (15 – 25)**

Score	Risk Rating
1 – 7	Low
8 – 14	Medium
15 - 25	High

To calculate the risk multiple the likelihood score by the impact score. For example

Example Risk Calculation				
Likelihood	**X**	**Impact**	**=**	**Risk**
2 (Unlikely)	X	3 (Possible)	=	6 (Low)

Identify Solutions to Mitigate Risks

For processing to begin, the risks that were identified need to be mitigated or removed. Some risks can be easily removed by abandoning an unnecessary aspect of the project. Certain aspects of the project could be abandoned if the risks out-weigh the benefits to the data subjects or the HSE. As every project and every PIA is different, there is no set way to mitigate all of the risks involved. The DPC has identified a number of possible solutions to mitigate a wide variety of data protection risks:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.

- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have.
- If you are using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

Section 5 – Data Subject Consultation

Consultation with data subjects (or a representative)

Under the GDPR, when carrying out a PIA, the controller shall seek the views of data subjects or their representative on the intended processing, where appropriate, and without prejudice to the protection of commercial or public interests or the security of processing operations.

Section 6 – DPO/DDPO Consultation

Obtain DPO/DDPO opinion

The DPO/DDPO can give their opinion on the PIA and highlight any issues that they feel may require attention. The rest of the form must be completed in its entirety before the DPO/DDPO can comment.

Consultation with the Commission needed?

If it appears to the controller, having conducted a data privacy impact assessment that the processing concerned would, despite the implementation of safeguards and security measures result in a high risk to the rights and freedoms of individuals then the controller must consult with the Data Protection Commission by request in writing prior to commencing the processing, via the DPO

The controller shall provide the DPO with the data privacy impact assessment conducted in relation to the processing concerned and any other information required to enable the DPO to liaise with the Commission and for the Commission to assess the potential risks to the rights and freedoms of individuals arising from the proposed processing. The Commission will issue written advice within a period of 6 weeks.

Section 7 – Approval

Can PIA be approved?

The controller will have to decide if the PIA provides sufficient information to sign off on the processing taking into consideration any written advice made by the Commission in cases where consultation has taken place. The controller should consider if the processing provides enough benefit to the data subjects to out-weigh the risk and if the solutions are sufficient to reduce the risks.

If the PIA is not signed off, the process may have to be reassessed or abandoned completely.

If the PIA is signed off, the processing can begin.