Data Protection Impact Assessment (DPIA) Template

Data Protection Impact Assessment Template

Background:
Data Protection Impact Assessments ('DPIAs') can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect SETU. DPIAs are mandatory for any new high risk processing projects.

When to use a DPIA:
Under the GDPR, a DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons/data subjects (the person to which the data relates). However, carrying out a DPIA is required as a standard practice in SETU and will serve as a useful tool to help comply with data protection law. The DPIA should be carried out prior to the processing of data and a copy sent to the Data Protection Officer to retain on file.

Who must carry out the DPIA:
It is the responsibility of the project team to ensure that a DPIA is carried out for any new high risk data processing projects.

DPIA Process:

1. **Need for DPIA:**
   Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified
2. **Describe the information flows:**
   Describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

3. **Identify data protection and related risks**
   Identify the key privacy risks and the associated compliance and corporate risks.

4. **Identifying data protection solutions to reduce or eliminate the risks**
   Describe the actions you could take to reduce the risks, and any future steps which would be necessary.
5. **Signing off on the outcomes of the DPIA**
   Ensure appropriate sign off of outcomes is formally documented and retained.

6. **Integrating data protection solutions into the project**
   Ensure the controls and actions identified are tracked through to completion to ensure the rights of the data subject are upheld.

Template

1. Need for a DPIA Please answer the below questions	
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used or in a way it is not currently used?	
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example,	

health records, criminal records or other information that people would consider to be private.	
Will the project require you to contact individuals in ways that they may find intrusive?	

2. Describe the information flows	
Date of Assessment:	
Assessment performed by:	
Function/Department:	
Process Name:	
Description of the envisaged processing operations: (Including collection, deletion and use)	
Purposes of the processing:	
Legal basis for processing:	
Necessity of the processing (Justification)	
Proportionality of the processing (Estimated number of Data Subjects Affected)	
Individuals consulted during the performance of DPIA (Include internal and external consultations held)	

3. Identify data protection and related risks			**4. Identifying data protection solutions to reduce or eliminate the risks**				
No.	Privacy Issue	Risk	Existing Controls Identified	Risk Rating L x I	Additional Controls/ Actions Required	Action Owner	Deadline Date
1							
5. Signing off on the outcomes of the DPIA							
DPIA Assessment result: (Pass- risk eliminated, avoided or accepted; Fail- risk unavoided)							
Approved by:							
6. Integrating data protection solutions into the project							
Next steps/Actions							

Guidance

Example Risks to Individuals:

- Inappropriate disclosure of personal data internally due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by “hackers”.
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.

- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- 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 purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Corporate Risks:

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
- Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of organisation's use of personal information may lead to a reluctance on the part of individuals to deal with the organisation.
- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your company keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against the organisation. Under the GDPR the organisation may also be liable for non-material damage.

Compliance Risks:

The organisation may face risks of prosecution, significant financial penalties, or reputational damage if it fails to comply with the GDPR. Individuals affected by a breach of the GDPR can seek compensation for both material and non-material damage.

Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Examples of data protection solutions:

- 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 with the organisation.
- If 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.

Risk Assessment Guidance:

Likelihood/Potential for an Incident to occur	Impact/Outcome of Incident	Risk Level Calculation L X I	Guideline Action Timetable
1 - Rare: No history of event occurring over period of years. This event may occur but in exceptional circumstances.	**1.** Minor compromise of privacy (e.g. un-sensitive personal data such as helpdesk ticket compromised)	1 – 2 Acceptable	No Action
2 - Unlikely: The event would be expected to occur annually	**2.** Minor data breach (e.g. inappropriate contact of data subject via email)	3 – 5 Low	Prioritise after medium risk actions complete
3 - Possible: This could occur monthly, as such it has a reasonable chance of occurring.	**3.** Moderate data breach (Sensitive data e.g. payroll compromised)	6 – 10 Medium	Prioritise after high risk actions complete
4 - Likely: Expected to occur at least weekly, the event will occur in most situations	**4.** Significant data breach (Financial loss, severe stress for a data subject or data subjects	11 – 15 High	Prioritise Action as soon as Practical
5 - Certain: Expected to occur almost daily, it is more likely to occur than not.	**5.** Major data breach (Risk of severe financial loss to a large number of data subjects)	16 – 25 Very High	Action Urgent