

Appendix 1

Data Protection Assessment Screening Form

The following questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops.

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 for, 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?

Appendix 2
Data Protection Assessment

Step one: Identify the need for a 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 (this can draw on your answers to the screening questions)

Step two: Describe the information flows

The collection, use and deletion of personal data should be described 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.

--

Consultation requirements
<p>Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.</p> <p>Consultation can be used at any stage of the DPIA process.</p>

Step three: identify the privacy and related risks	
<p>Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.</p> <p>Annex three can be used to help identify GDPR related compliance risks</p>	
Privacy issue	

Risk to individuals	
Compliance risk	
Associated organisation / corporate risk	

Step four: Identify privacy solutions	
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).	
Risk	
Solutions	
Result: is the risk eliminated, reduced, or accepted?	
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	

Step five: Sign off and record the DPIA outcomes
Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Step six: Integrate the DPIA outcomes back into the project plan	
Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?	
Action to be taken	
Date for completion of actions	
Responsibility for action	

Contact point for future privacy concerns	
---	--

Appendix 3

Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help identify where there is a risk that the project will fail to comply with GDPR or other relevant legislation, for example the Human Rights Act.

1st Principle: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). In particular, shall not be processed unless: a) at least one of the conditions in GDPR Article 6 is met, and b) in the case of special category personal data, at least one of the conditions in GDPR Article 9 is also met.

- Have you identified the purpose of the project?
- How will individuals be told about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to the Human Rights Act, you also need to consider:
- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

2nd Principle: 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\(1\)](#), not be considered to be incompatible with the initial purposes ('purpose limitation');

- Does your project plan cover all of the purposes for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?

3rd Principle: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- Is the information you are using of good enough quality for the purposes it is used for?
- Which personal data could you not use, without compromising the needs of the project?

4th Principle: 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 ('accuracy');

- If you are procuring new software does it allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?

5th Principle: 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 ('storage limitation');

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software which will allow you to delete information in line with your retention periods?

6th Principle: 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 ('integrity and confidentiality').

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?