Data Protection Impact Assessment – the ICO seven steps

A Data Protection Impact Assessment should be completed at the start of any significant service change or project involving the use of personal data, or if making changes to an existing process. The final outcomes should be integrated back into any project plans.

Such changes could include:

- introduction of new technologies, applications or systems;
- changes to the way that personal information is being used;
- use of automated processing of personal information;
- outsourcing of use of personal information;
- new sharing initiative involving personal information.

This DPIA should be completed by the project lead. Others associated with the project may also need to contribute, such as front line, ICT, HR or procurement staff.

The Information Management Team can assist with any queries and will receive and sign-off once completed.

Service name	
Service change / project	
Completed by	
Completion date	
Approved by Information Management	
3-yearly review date	
Date shortlisting due to take place	
Date contract due to be awarded	

Step 1 - identify the need for a DPIA Explain broadly what the service/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. (Your answers to the DPIA screening questions may be useful here).

Step 2 - describe the processing **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone, or using data shared with you? You might find it useful to refer to a flow diagram or other way of describing information flows. What types of processing identified as likely to be high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing, for you and more broadly?

Step 3 - consultation process Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views, or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? Who might you need to involve outside your organisation, or in partner organisations? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4 - assess necessity and proportionality Describe compliance and proportionality, in particular what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step Five - identify and assess risks			
Describe sources of risk and the nature of potential impacts on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6 - integrate the DPIA outcomes back into the project plan

Identify additional measures you could take to reduce or eliminate risks identified in Step 5.

Risk	Mitigations to reduce or eliminate risk	Effect on the risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7 - sign-off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into the project plan, with date and responsibility for completion.
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead.
DPO advice provided:		The DPO should advise on compliance, Step 6 measures, and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA.

Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help you to identify any risks that the project may fail to comply with the Data Protection Act 2018 (DPA2018) and the General Data Protection Regulations (GDPR), or other relevant legislation such as the Human Rights Act. Each principle is listed below with a checklist of bullet points for each one.

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime and requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

- We have clearly identified our purpose or purposes for processing.
- We have documented those purposes.
- We include details of our purposes in our privacy information for individuals.
- We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

(b) 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 not be considered to be incompatible with the initial purposes ('purpose limitation');

- We will only collect personal data we actually need for our specified purposes.
- We have sufficient personal data to properly fulfil those purposes.
- We periodically review the data we hold and delete anything we don't need.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- We only collect personal data we actually need for our specified purposes.
- We have sufficient personal data to properly fulfil those purposes.
- We periodically review the data we hold, and delete anything we don't need.

(d) 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');

- We ensure the accuracy of any personal data we create.
- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

(e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

- We know what personal data we hold and why we need it.
- We carefully consider and can justify how long we keep personal data.
- We have a policy with standard retention periods where possible, in line with documentation obligations.
- We regularly review our information and erase or anonymise personal data when we no longer need it.
- We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
- We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

(f) 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')."

- You must ensure that you have appropriate security measures in place to protect the personal data you hold.

- This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

  More detailed information regarding security can be found on the ICO website.

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

  - This specifically requires you to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that you comply

  More detailed information regarding the accountability principle can be found on the ICO website.