TEMPLATE DATA PROTECTION IMPACT ASSESSMENT

Data protection impact assessment template

This template is an example of how you can record the DPIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a DPIA. This template broadly follows the process used in the ICO Code of Practice.

Consultation: The Code recommends that consultation should be undertaken as necessary with all stakeholders throughout the DPIA process. The Data Protection Officer ("DPO") should be consulted at the first opportunity. The DPO will provide guidance on the correct completion of the DPIA.

Completed DPIA's must be lodged with the DPO as soon as possible and in no case later than one month before the "go live" date of the project.

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.* Further information: Read p. 20-21 of ICO Code of Practice

Step two: Describe the information flows *You should 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.* Further information: Read p. 22 of ICO Code of Practice

Step three: Linking the DPIA to the data protection principles *Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.*
Principle 1 *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:* *a) at least one of the conditions in Schedule 2 is met, and* *b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.* **How will you tell individuals about the use of their personal data?**

Do you need to amend the privacy notices?

Have you established which conditions for processing apply? (See ICO guidance for details)

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are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act? (See Chapter 8 text for details)

Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

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?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

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?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Step four: Identify the privacy and related risks
Based on your responses to the screening questions and step 3 above, 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.

Further information: Read p. 23-26 of ICO Code of Practice

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step five: Identify privacy solutions
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Further information: Read p. 27-29 of ICO Code of Practice

Risk	**Solution(s)**	**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 six: Sign off and record the DPIA outcomes
Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Further information: Read p. 30-31 of ICO Code of Practice

Risk	**Approved solution**	**Approved by**

Step seven: 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 that may arise in the future?

Further information: Read p. 32 of ICO Code of Practice

Action to be taken	**Date for completion of actions**	**Responsibility for action**

Mrs S C Grant
Secretary and Registrar
Signed: **25 May 2018**