**Data Protection Impact Assessment**

This assessment requires prior completion of a Data Protection Impact Assessment Screening Questionnaire.

This should be completed by one or more members of the project in collaboration with, or with the assistance or support of, Information Governance.

Please refer to the ICO guidance on conducting Data Protection Impact Assessments for more detailed methodology, if required:

<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/>

**Project /procedure/change :**

**Completed by (Institute/section/dept.) :**

**Date :**

**Reviewed and confirmed by Data Protection Manager/their nominee:**

**Date :**

**Step one:** Identify the need for a DPIA

Using the responses to the screening questions as the basis, summarise how and why the need for a DPIA was identified

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. Arrange and number the section below as appropriate.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Step two (i):** Describe the information flows

The collection, use, deletion and any other processing of personal data should be described here and it may also be useful to refer to a flow chart, diagram or another way of explaining data flows. Refer to IT infrastructure where relevant. You should also say how many individuals are likely to be affected by the project.

*e.g. Data will be collected from research participants via online forms*

*↓*

*Data will be stored encrypted on secure shared drives*

*↓*

*Pseudonymised dataset will be provided to X along with report*

**Step two (ii):** Describe the consultation process

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.

|  |  |
| --- | --- |
| Consultation requirements |  |
| Internal consultation (within Department/Institute) |  |
| Internal consultation (other Department/Service Department/Committee advisory officer, etc.) |  |
| External consultation (e.g. service supplier, sector advisory bodies, professional organisations) |  |

**Step three:** identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

**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).

Steps 3 and 4 can be combined in the suggested table below. Use a separate sheet/document if necessary.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Log/ Risk No** | **Privacy or compliance risk**  **(to individuals/ to institution)** | **Mitigation/solution** | **Result (e.g. is risk reduced, accepted, eliminated)** | **Evaluation (is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?)** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |

**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?

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.** | **Description of Risk** | **Approved Solution** | **Approved by** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**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 for future privacy concerns:**

**APPENDIX**

**Linking the DPIA to the data protection principles**

Answering some of these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with data protection 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.**

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?

**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 potential new purposes been identified 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 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?

**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 which 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?