Privacy Impact Assessment

Project Name:

# Stage 1 – PIA Screening Questions

Answering ‘Yes’ to any of these would indicate that a full PIA would be useful.

|  |  |  |
| --- | --- | --- |
|  | No | Yes |
| 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? |[ ] [ ]

# Stage 2 – Privacy Impact Assessment

## Identify the need for a PIA

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 PIA was identified (this can draw on your answers to the screening questions).

## 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.

## Consultation Requirements

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.

You can use consultation at any stage of the PIA process.

## Identify 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.

Stage three can be used to help you identify the DPA related compliance risks.

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy Issue | Risk to Individuals | Compliance Risk | Associated Organisation / Corporate Risk |
|  |  |  |  |

## 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 | Solution(s) | Result | Evaluation |
|  |  |  |  |

Result: is the risk eliminated, reduced to accepted?

Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

## Sign-off and Record the PIA Outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

|  |  |  |
| --- | --- | --- |
| Risk | Approved Solution | Approved By |
|  |  |  |

## Integrate PIA Outcomes back into the Project

Who is responsible for integrating the PIA 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?

|  |  |  |
| --- | --- | --- |
| Action to be taken | Date for completion of actions | Responsibility for actions |
|  |  |  |

# Stage 3 – Link PIA to Data Protection Principles

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| Principle 1Personal 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, andb) 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 you tell individuals 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? |[ ] [ ]   |
|  |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| Principle 2Personal 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? |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| Principle 3Personal 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? |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| 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? |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| Principle 5Personal 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? |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| 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? |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| Principle 7Appropriate 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? |[ ] [ ]   |

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | Yes | Comments |
| 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? |[ ] [ ]   |