**Privacy Impact Assessment**

**Name of Project:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Privacy and data protection is a key consideration in the early stages of any project and throughout its life cycle.**

**Examples of projects that would require a PIA include (but are not limited to):**

* A new IT system for storing and accessing personal data.
* A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
* A proposal to identify people in a particular group or demographic and initiate a course of action.
* Using existing data for a new and unexpected or more intrusive purpose.
* A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
* A new database which consolidates information held by separate parts of an organisation.
* Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

**GDPR Committee members / GDPR Champion:**

* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Project Committee members:**

* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Privacy impact assessment screening questions**

These questions are intended to help decide whether a PIA is necessary. Answering ‘yes’ to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

|  |  |
| --- | --- |
|  | **Yes /No** |
| **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 which 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 which 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 particularly private.** |  |
| **Will the project require you to contact individuals in ways which they may find intrusive?** |  |

|  |  |
| --- | --- |
| **Information the PIA needs to contain** | **Please complete this column in full or reference and attach the documentation containing the required information** |
| **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:** The collection, use and deletion of personal data needs to be described.  [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.  [Consultation can be used at any stage of the PIA process and is not a defined step in the process] |  |
| **Identify the Privacy and related risks:-**  Identify the key privacy risks and the associated compliance and corporate risks.  [It might be useful to record this information on a more formal risk register. Answering the questions in Annex 1 will help identify where the project will not comply (based on Data Protection Bill Principles)] |  |
| **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. Annex 2 may assist in the layout] |  |
| **Sign off the PIA**  Who has approved the privacy risks involved in the project? What solutions need to be implemented?  [Each risk needs to be identified alongside the solution and a signature approving the solution. This needs to be signed off at a senior level, it is not a department matter. Annex 3 may assist] |  |
| **Integrate the PIA Outcomes back into the project plan:**  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 which may arise in the future? |  |
| **Contact for Future Privacy Concerns** |  |
| **This document should be circulated to all those listed at the top of the document and a record retained that the document has been circulated. When the project is under review this document should be revisited.** | |

This document needs to be signed off at senior level and by those involved in the project and by the nominated persons responsible for GDPR. A signed copy should be retained with the project information and by the GDPR committee.

By signing below you are confirming that you have read and agreed with the content of this PIA. If there are any areas of concern they need to be raised, revisited and documented.

**Board Member with responsibility for GDPR as identified in roles and responsibilities:**

* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**GDPR Committee members:**

* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Project Committee members:**

* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Annex One**

Linking the PIA to the 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 Data Protection Bill or other relevant legislation, for example the Human Rights Act.

**Principle 1**

**The processing of Personal Data must be lawful, fair and transparent. In particular, Personal Data shall not be processed unless:**

1. **at least one of the conditions in Schedule 9 is met, and**
2. **in the case of sensitive personal data, at least one of the conditions in Schedule 10 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, explicit and legitimate 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 must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing data. These risks include but are not limited to: accidental or unauthorised access to or destruction, loss, use, modification or disclosure of 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?

**Transferring Data outside the EU**

* 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?

**Annex Two**

|  |  |  |  |
| --- | --- | --- | --- |
| **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? |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Annex three**

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