**DATA PROTECTION IMPACT ASSESSMENT**

**CONTENTS**

* **Introduction**
* **Do I need to undertake a Privacy Impact Assessment (PIA)**
* **Privacy Impact Assessment Template**
* **Assessment of Risk and Sign- Off**

**INTRODUCTION**

A Privacy Impact Assessment (PIA) is a process designed to help you systematically analyse, identify and minimise the data protection risks of a procurement, project, plan or type of processing. It is a key part of your accountability obligations under data protection legislation, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations. It should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve. It should be an ongoing processes that helps you monitor whether your process remain complaint.

This document provides you with a template for a Privacy Impact Assessment. It also provides you with guidance and examples on what should be considered

**DO I NEED TO UNDERTAKE A PIA**

You **must** carry out a PIA when:

* using new technologies; and
* the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

* systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
* large scale processing of special categories of data or personal data relation to criminal convictions or offences. This includes processing a considerable amount of personal data that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
* large scale, systematic monitoring of public areas (e.g. CCTV).

Further guidance on what could constitute high risk and large scale is available on the ICO website. <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/>

You **are encouraged** to carry out a PIA if you answer ‘yes’ to any of the following questions because it will help the council to demonstrate compliance with data protection legislation:

* + - * Will the process / project involve the processing of information about individuals?

##### Will the process / 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?

##### Will you be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

##### Will the Personal Data be used for direct marketing? E.g. to tell people about council services.

##### Will the process / project require you to contact individuals in ways which they may find intrusive?

##### **PRIVACY IMPACT ASSESSMENT TEMPLATE**

##### This PIA template is for Project managers and Service Managers This PIA records the results of your assessment and how your project or review of or changes to an existing process complies with the requirements of the data protection legislation and delivers the identified outcomes for the project or review.

##### You should try to start the PIA from the beginning of a procurement, project or the reviewing or changing of an existing process that involves the collecting, storing, disclosure, sharing and/or disposal of data.

|  |  |
| --- | --- |
| **1.** | **Name of the Information Asset Owner** |
|  |  |
| **2.** | **Name of the procurement, project / service function;** ***e.g. a new building with a CCTV, review of an existing data collection process, a new customer booking form (online or paper),*** |
|  |  |
| **3.** | **Describe the procurement, project / service function**  **e.g.** **explain what the new / reviewed process or project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.** |
|  | The aims of the project are:- |
|  | Relevant documents are linked here. |
|  | A PIA is required because: |
| **4.** | **Describe the processing/information flows**  **e.g. The collection, use and deletion of personal data should be described 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 new / reviewed process or project aims to achieve.** |
|  | We will collect the following Personal Data (names, addresses, card details, images) |
|  | If applicable - We will collect the following special categories of Personal Data :   * racial or ethnic origin * political opinions * religious or philosophical beliefs * trade union membership * the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person * data concerning health or data concerning a natural person's sex life or sexual orientation |
|  | The data flow looks like this: [ insert ] |
|  | The processing will involve XX number of people.   * XX % are children * XX% are vulnerable groups or individuals |
|  | Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual? |
|  | Does the project involve new or significantly changed handling of personal data about a large number of individuals? |
|  | Does the project involve new or significantly changed consolidation, inter-linking, cross- referencing or matching of personal data from multiple sources? |
| **5.** | **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 new / reviewed process or project aims to achieve management Outcomes. Consider any statutory requirement the council has to consult on service provision.** |
|  | We will consult the following people internally: |
|  | We will consult the following people externally: |
|  | We will seek views from individuals by: |
|  | We are required to carry out the following statutory consultation as part of this project: |
|  | The Consultation will be carried out in the following way and in the following timescale: |
| **6.** | **Identifying Risks** |
| **6.1** | **The Data Protection Principles**  **Answering questions during the PIA process about how your project or process review complies with the data protection Principles will help you to identify where there are risks and solutions to mitigating them.** |
|  | **Principle 1- Lawfulness, fairness and transparency** |
|  | How will individuals be told about the use of their personal data? |
|  | What processing condition applies to this processing?  e.g. contractual |
|  | What processing condition applies to the special categories of personal data being collected?  e.g. consent |
|  | Will your actions interfere with the right to privacy?  e.g. will you be data matching without consent  If yes explain how:  This interferences is justified because: |
|  | **Principle 2- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with 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? |
|  | Have you updated the list of processing held by the council?  List the purpose(s) for the processing here: |
|  | If the project involves direct marketing, what process do you have in place to collect the personal data for that purpose?  We will demonstrate consent for marketing by:  Data Subjects can withdraw their consent by: |
|  | **Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed** |
|  | Explain how you could you minimise the Personal data you want to collect, without compromising the needs of the project? |
|  | Explain how you could you anonymise or pseudonymised the personal data, without compromising the needs of the project? |
|  | How will you prevent information creep during the processing? |
|  | What measure will you put in place to ensure that processor comply with data protection legislation? |
|  | **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 or add data when necessary? |
|  | How will you ensure the accuracy of the data you are collecting? |
|  | How will you ensure the quality of the data you are processing? |
|  | How will you ensure the personal data is kept accurate and up to date where necessary? |
|  | **Principle 5- Personal data shall be 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** |
|  | What retention periods are suitable for the personal data you will be processing? |
|  | Explain how the software will allow you to delete information in line with your retention periods |
|  | Explain how the software will allow you to set retention period on documents in line with your retention periods? |
|  | What manual process do you have in place to ensure that personal data is not being kept longer than is necessary? |
|  | **Principle 6 - Personal data shall be 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** |
|  | Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?  e.g. radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic |
|  | Do any new systems provide protection against the security risks you have identified? |
|  | How will the personal data be secured? |
|  | How much control will the data subject have over their data? |
|  | Will Data subject expect this processing? |
|  | Is this a novel way of processing? |
|  | What is the current state of the technology for this type of processing? |
|  | Are there any prior concerns regarding this processing? |
|  | Are there any public concerns about this type of processing? |
| **6.2** | **Joint Working** |
|  | Does the project involve multiple organisations, whether they are other councils, government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations? If Yes please explain;  e.g.   * Are there joint Controllers of the personal data? * Is a data sharing agreement required? * Is a processing agreement required? |
|  |  |
| **6.3** | **Processing in accordance with the rights of data subjects under GDPR** |
|  | What arrangements will you put in place to address data subject rights:Right to be informedRight to accessRight to rectificationRight to forgotten/erasureRight to object and restrict processingRight to data portabilityRight in relation to international transfersRights in relation to automated decision-making and profiling |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ASSESSMENT OF RISKS** | | | | | |
| **Identify the key privacy risks (assign each risk a reference number) and the associated compliance risk and corporate risks.**  **When assessing the impact try to score over the range 1 to 10**  **1 to 3 low**  **4 to 6 Medium**  **7 to 10 High** | | | | | |
| **Risk**  **No.** | **Risk to Data Subject** | **Level of Risk** | **Solution** | **Result of Solution (resolved, reduced or unresolved)** | **Level of Risk after Result of Solution**  **(if High consult ICO)** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | **SIGN OFF AND RECORD OF OUTCOMES** | | | | |
| **Risk**  **No.** | **Approved by**  **SIRO/Information Asset Owner** | **Name/ Date** | | | |
|  |  |  | | | |
|  |  |  | | | |
|  | **Advice of DPO provided** |  | | | |
|  | **Summary of DPO advice:** | | | | |
|  | **Advice of DPO accepted or overruled** | **If Overruled you must explain your reasons** | | | |
|  | **Comments** | | | | |
|  | **Integrate the PIA outcomes back into the project plan** | | | | |
|  |  | | | | |