Privacy Impact Assessment – GDPR10

As part of the PIA process organisations should describe how information is collected, stored, used and deleted.

Project Name	

What is the Projects Outcome	
Information to be obtained	
What is the information to be used for?	
Who will obtain it?	
Who will have access to the information?	
Any other Information?	
Identify Possible Privacy Risks Risks to individuals, Corporate Risks, Compliance Risks, Associated Organisation/Corporate Risk	
Identify how to mitigate these Risks Risk, Solution, Result and Evaluation.	
Evaluate costs involved	
Recourses required for the project	
Review Process Who will action the review? When will it be reviewed? Action to be take Date for completion Responsibility for action. Lessons learnt	

What to think about when preparing the Privacy Impact Assessment.
This form is to be used in conjunction with Conducting Privacy Impact Assessments Code of Practice.

It can be integrated with consultation or planning processes. Effective consultation internally within the Council is an important part of any Privacy Impact Assessment (PIA) .PIA. Data protection risks are more likely to remain unmitigated on projects which have not involved discussions with the people building a system or carrying out procedures.

Screening questions to help you decide whether a Privacy Impact Assessment is required:
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?

When preparing your Privacy Impact Assessment you need to identify the below possible Stake holders.

- Project management team
  The team responsible for the overall implementation of a project will play a central role in the PIA process.

- Data protection officer
  If an organisation has a dedicated DPO, they are likely to have a close link to a PIA. Even if project managers are responsible for individual PIAs, the DPO will be able to provide specialist knowledge on privacy issues,

- Engineers, developers and designers
  The people who will be building a product need to have a clear understanding of how to approach privacy issues. They will also be able to suggest workable privacy solutions to the risks which have been identified.

- Information technology (IT)

Will be able to advise on security risks and solutions. The role of IT is limited to security, and might also include discussions on the usability of any software.

- Procurement
  If the project will require systems or services to be procured, the needs of the project need to be established before procurement takes place.

- Potential suppliers and data processors
  If some of the project will be outsourced to a third party, early engagement will help to understand which options are available.

- Communications
  A PIA can become a useful part of a project's communication strategy. For example, involving communications colleagues in the PIA can help to establish a clear message to the public about a project.

- Customer-facing roles
  It is important to consult with the people who will have to use a new system or put a policy into practice. They will be able to advise on whether the system will work as intended.

- Corporate governance/compliance
  Colleagues who work on risk management for an organisation should be able to integrate PIAs into their work. Other areas of compliance can be included in the PIA process.

- Researchers, analysts, and statisticians
  Information gathered by a new project may be used to analysing customer behaviour or for other statistical purposes. Where relevant, consulting with researchers can lead to more effective safeguards such as anonymisation.

- Senior management
  It will be important to involve those with responsibility for signing off or approving a project.

External Consultation

External consultation means seeking the views of the people who will be affected by the project. This may be members of the public, but can also mean people within an organisation (for example staff who will be affected by a new online HR system). Consultation with the people who will be affected is an important part of the PIA process. There are two main aims. Firstly, it enables an organisation to understand the concerns of those individuals. The consultation will also improve transparency by making people aware of how information about them is being used.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how

information is used can be a significant privacy risk – for example; data might be used for unfair purposes, or disclosed inappropriately.

You must have regard when linking to the Privacy Impact Assessment to the 8 Data Protection principals below:

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?