

PRIVACY IMPACT ASSESSMENT TEMPLATE

Privacy impact assessment screening questions

These questions are intended to help you 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.

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?

Privacy impact assessment template

The template follows the process that is used in the ICO's PIA code of practice.

Step one: 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).

Step two: 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.

Step three: Identify the privacy and related risks

Definition of personal data:

Data which relate to a living individual who can be identified –

- (a) from those data, or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Definition of sensitive personal data:

Personal data consisting of information as to –

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union,
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The 8 Data Protection Principles:

1. Personal data shall be processed fairly and lawfully
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.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
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.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

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.

Principle 1 - Personal data shall be processed fairly and lawfully

Privacy issue	Comments
Have you identified the purpose of the project?	
Is there a lawful reason you can carry out this project?	
How will you tell individuals about the use of their personal data?	
Do you need to amend your privacy notices? The Council's main one can be found here . Do you have service specific ones?	
Have you established which schedule 2 conditions for processing apply? (The conditions can be found here .)	
If sensitive personal data is involved, have you established which schedule 3 conditions for processing apply? (The conditions can be found here .)	
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?	
Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act ? If yes, is it necessary and proportionate?	
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

Privacy issue	Comments
Does your project plan cover all of the purposes for processing personal data?	
Which personal data could you not use, without compromising the needs of the project?	

Principle 3 - Personal data shall be adequate, relevant and not excessive

Privacy issue	Comments
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?	

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date

Privacy issue	Comments
If you are procuring new software does it allow you to amend and / or delete 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 is necessary

Privacy issue	Comments
What retention periods are suitable for the personal data you will be processing? How long will you keep the data for?	
Are you procuring software that 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

Privacy issue	Comments
What process is in place to answer 'Subject Access Requests' (requests for personal data)?	

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.

Privacy issue	Comments
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?	
What training on data protection and / or information sharing has been undertaken by relevant staff?	

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection.

Privacy issue	Comments
Will the project require you to transfer data outside of the EEA? If yes how does it demonstrate an adequate level of protection?	
If you will be making transfers outside of the EEA, how will you ensure that the data is	

transferred securely?

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

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?

Step five: 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

Step six: 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 that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

For further information or guidance, see the ICO's website at www.ico.gov.uk

Privacy Impact Assessment – Guidance

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary

Corporate Risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Reducing the risks

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. The costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.