Information Commissioner's Office

Conducting privacy impact assessments code of practice

Data Protection Act

Contents

About this code

Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

This code explains the principles which form the basis for a PIA. It sets out the basic steps which an organisation should carry out during the assessment process. The code also contains a set of screening questions to help organisations identify when a PIA is necessary, and a template which can be used to help produce a PIA report.

The code will be useful for any organisation which is thinking about conducting a PIA. The process described in the guidance is designed to be flexible enough to work for organisations of any size and in any sector.

Many organisations, particularly those which conduct regular PIAs, may find it useful to develop their own PIA process with accompanying guidance. This code can be used as a starting point to develop a methodology which fits with the organisation's own needs and working practices.

The ICO will also support sectoral groups who wish to develop a PIA methodology to apply to their particular sector. For example, sectors might find it useful to develop a more specific set of screening questions or identify common privacy risks and solutions.

The Information Commissioner has issued this code of practice under section 51 of the Data Protection Act (DPA) in pursuance of his duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act. Conducting a PIA is not a requirement of the Act, but undertaking one will help to ensure that a new project is compliant.

Chapter 1 - Introduction to PIAs

Key points:

- A PIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.

- Conducting a PIA involves working with people within the organisation, with partner organisations and with the public to identify and reduce privacy risks.

- The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

- Conducting a PIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.

What the ICO means by PIA

A PIA enables an organisation to analyse how a particular project or system will affect the privacy of the individuals involved.

The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

A PIA will help ensure that an organisation is taking a proportionate approach to the use of personal data. It requires organisations to identify why a project is necessary and what it is aiming to achieve. The PIA will then help to achieve these aims without a disproportionate impact on privacy.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

The ICO has designed its PIA methodology to be as flexible as possible so that it can be integrated with an organisation’s existing ways of working.

What do we mean by privacy?

A PIA is designed to go further than a straightforward compliance check against the DPA or other legislation. A compliance check is more likely to focus on ensuring that any processing of personal data complies with the DPA and other relevant legislation. A PIA should go beyond this and include a wider understanding of privacy concerns. In particular a PIA should prompt organisations to think about a project from the perspective of the individuals affected.

As the DPA is the key driver of PIAs, privacy of personal data will lie at the core of the assessment but focusing on the general concept of privacy will bring many benefits. And it is more efficient for organisations to address privacy risks in one process.

Issues to be considered in the context of privacy include:

- Expectations of how the activity of individuals will be monitored.
- Expectations of the level of interaction between an individual and an organisation.
- An understanding of how and why particular decisions are made about people.

Public bodies also need to be aware of their obligations under the Human Rights Act. Article 8 of the European Convention on Human Rights guarantees a right to privacy which can only be interfered with when it is necessary to meet a legitimate social need. Organisations which are subject to the Human Rights Act can use a PIA to help ensure that their actions are a proportionate response to a legitimate aim.

The benefits of a PIA

Conducting a PIA is not a legal requirement of the DPA. The ICO promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits. Carrying out an effective PIA should benefit the people affected by a project and also the organisation carrying out the project.

The first benefit to individuals will be that they can be reassured that the organisations which use their information have followed best practice. A project which has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A second benefit to individuals is that a PIA will improve transparency and make it easier for them to understand how and why their information is being used in a particular way.

Organisations that conduct effective PIAs should also benefit. The process of conducting the assessment will improve how they use information which impacts on individual privacy. This should in turn reduce the likelihood of the organisation failing to meet its legal obligations under the DPA and of an unauthorised disclosure of personal data occurring.

Conducting and publicising a PIA will help an organisation to build trust with the people using their services. The actions taken during and after the PIA process can improve an organisation's understanding of their customers.

There are financial benefits to conducting a PIA, identifying a problem early will generally require a simpler and less costly solution. A PIA can also reduce the on-going costs of a project by minimising the amount of information being collected or used, where this is possible and devising more straightforward processes for staff.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of a project.

Projects which might require a PIA

The core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

PIA terminology often refers to a project as the subject of a PIA and this should be widely construed. A PIA is suitable for a variety of situations:

- 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 new policy which will 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 PIA should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that PIAs are more likely to be of use when applied to new projects or revisions of existing projects. Conducting a PIA of an existing project is less likely to make a positive difference unless it is possible for necessary changes to be implemented.

Organisations should try to identify the need for a PIA at an early stage and should consider building this into their project management policies.

Chapter 2 - The PIA process

Key points:

- The PIA process is a flexible one that can be integrated with an organisation's existing approach to managing projects
- A PIA should begin early in the life of a project, but can run alongside the project development process
- A PIA should incorporate the following steps:
    - Identify the need for a PIA
    - Describe the information flows
    - Identify the privacy and related risks
    - Identify the privacy solutions
    - Sign off and record the PIA outcomes
    - Integrate the outcomes into the project plan
    - Consult with internal and external stakeholders as needed throughout the process

The PIA process is a flexible one, and it can be integrated with an organisation's existing approach to managing projects. This guidance identifies the key principles of PIAs which the ICO suggests should be included.

Many organisations will benefit from producing their own PIA process and accompanying guidance. This is often the most effective way of ensuring that privacy issues are considered as part of the existing project or risk management procedures and that the PIA covers any sectorial or organisational specific angles. Annex four explains how organisations can integrate PIAs with project and risk management.

The process of conducting a PIA should begin early in the project. When it becomes clear that a project will have some impact on privacy an organisation should start to consider how they will approach this. This does not mean that a formal PIA must be started and finished before a project can progress further. The PIA should run alongside the project development process. What begins as a more informal early consideration of privacy issues can be developed into part of the PIA.

Annex two provides a template which organisations can use to record the results of each of the steps detailed below. Organisations do not have to use the template and can chose to use existing records management systems or project management tools if they prefer.

Overview of the PIA process

1. Identifying the need for a PIA.

The need for a PIA can be identified as part of an organisation's usual project management process or by using the screening questions in annex two of this Code.

2. Describing the information flows.

Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information

3. Identifying the privacy and related risks.

Some will be risks to individuals - for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.

Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the DPA, PECR, and the Human Rights Act.

4. Identifying privacy solutions.

Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

5. Signing off and recording the PIA outcomes.

Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.

A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

6.Integrating the PIA outcomes back into the project plan.

The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.

Record what you can learn from the PIA for future projects.

Consultation with relevant stakeholders should take place during each stage.

Chapter 3 – Consultation

Key points:

- Consultation is an important part of a PIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise.
- Consultation can take place at any point in the PIA process.
- Internal consultation will usually be with a range of internal stakeholders to ensure that all relevant perspectives are taken into account.
- External consultation provides the opportunity to get input from the people who will ultimately be affected by the project and to benefit from wider expertise.

Consultation is an important part of a PIA, but organisations do not need to see it as a separate step. It can be useful to build consultation into all stages of the PIA process. This allows organisations to consult the right people at the right time and avoid having to spend more time and resources on a separate exercise.

Consultation allows people to highlight privacy risks based on their own area of interest and expertise. It also provides an opportunity for them to suggest measures to reduce the risks.

Internal consultation

Effective consultation with colleagues is an important part of any PIA. Data protection risks are more likely to remain unmitigated on projects which have not involved discussions with the staff who will be building a system or carrying out procedures.

Identifying a full range of internal stakeholders will be easier if you have already described the information flows in detail; but you may also need to do some initial internal consultation in order to describe the information flows in the first place.

Examples of internal stakeholders

- Project management team
  - The team responsible for the overall implementation of a project will play a central role in the PIA process.
- 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 not 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.
- Senior management
  - It will be important to involve those with responsibility for signing off or approving a project.

There is no set process for conducting internal consultation – it will depend on various factors, particularly the size of the organisation and the scale of the project. The PIA can be integrated with other consultation or planning processes.

External consultation

Consultation with the people who will be affected by a project 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.

How extensive the consultation needs to be will be driven by the types of risk and the numbers of people affected.

The consultation should be designed so that individuals can have a meaningful impact on the project. An organisation should be clear about which aspects of the project are open to change and which aspects are less so. It may be effective just to consult one aspect or targeted aspects. Any general public consultation must be set out in clear terms that can be easily understood. Public consultation can be an effective way to communicate with people about how you use their information.

An organisation may already have consultation mechanisms such as: focus groups, user groups, public meetings and consumer or citizen panels that can be used.

External consultation also provides the opportunity for organisations to benefit from wider views and from expertise that may not exist within the organisation itself.

Effective external consultations should follow these principles:

- Timely – at the right stage and allow enough time for responses.
- Clear and proportionate– in scope and focused.
- Reach and representative - ensure those likely to be effected have a voice.
- Ask objective questions and present realistic options.
- Feedback – ensure that those participating get feedback at the end of the process.

Chapter 4 – Identifying the need for a PIA

Key points:

- The need for a PIA can be identified as part of an organisation's normal project management process.
- The ICO has devised some simple screening questions to help organisations identify when a PIA is needed and we would encourage organisations to incorporate these questions into their own project management methodologies or procedures
- The screening questions are designed to be used by project managers or other staff who are not experts in privacy matters or data protection.

The first step in the PIA process will be identifying the need for a PIA. Annex one contains suggested screening questions which are designed to help organisations decide whether a PIA is necessary. They are designed to be used by project managers or other staff who are not experts in data protection or privacy matters.

The idea is that the screening questions will allow non-experts to identify the need for a PIA as part of the organisation's normal project management procedures. The PIA can then be completed with input from specialists within the organisation (such as compliance managers) if necessary.

We would encourage organisations to incorporate the screening questions into their own project and risk methodologies or procedures. Organisations can give preliminary answers to the questions at an early stage of the project and these can be expanded upon as the work develops.

Organisations can also develop their own screening questions to address the specific needs of the organisation if they wish. The most important thing is that organisations have some mechanism within their normal project management procedures for identifying the need for a PIA.

Later stages of the PIA process require an organisation to consider whether the impact on privacy is proportionate to the outcomes which will be achieved. At this early stage the organisation should be able to identify why the project is being planned and what the project is intending to achieve.

Not all projects will require the same level of PIA; there is a greater impact on privacy when data is sensitive or when its uses are more intrusive. However, most projects will benefit from a systematic analysis of how they will use personal data. The level of detail can be decided by the organisation and will depend on various factors, including the time and resources available to the project team.

Organisations do not need to worry at length about the scale of a PIA. A well-implemented PIA process can sit alongside a project of any size. The range of activities carried out as part of the project process will match those required for an effective PIA.

When a need for PIA is identified it is important that senior management support is sought for conducting the PIA. Gaining this commitment at an early stage is an important factor in ensuring the PIA is effective.

Chapter 5 - Describing information flows

Key points:

- Understanding the information flows involved in a project is essential to a proper assessment of privacy risks.
- Existing processes and resources such as information audits and information asset registers can be useful tools in completing this step of a PIA.

A description of the types and uses of personal information which come within the scope of the project is a key part of any PIA process. 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. As part of the PIA process organisations should describe how information is collected, stored, used and deleted. They should explain what information is used, what it is used for and who will have access to it.

Many organisations already conduct information audits and make use of information asset registers. This part of the PIA process can be integrated with any similar exercises which would already be done. If an organisation has already produced a project proposal or similar document it can be useful for understanding how personal data might be used.

The information flows can be recorded in whichever format meets the needs of your organisation (a flowchart, an information asset register, a project design brief) and this can then be used as an important part of your final PIA report. The PIA template at Annex two can also be used to record information flows.

Chapter 6 - Identifying privacy and related risks

Key points:

- When conducting a PIA an organisation should identify any privacy risks to individuals, compliance risks and any related risks for the organisation; such as fines for non-compliance with legislation or reputational damage leading to loss of business.

- Organisations may wish to use their existing project management or risk management methodologies to help them identify risks.

- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.

- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.

- The ICO's codes of practice on privacy notices and CCTV, as well as other more specific guidance, will also help you to focus PIAs on those issues.

- Organisations might also be able to refer to industry standards and guidance produced by trade bodies, regulators or other organisations working in their sector.

At this stage, organisations should assess the likely privacy issues associated with the project.

A key principle of PIA is that the process is a form of risk management. When conducting a PIA an organisation is systematically considering how their project will affect individuals' privacy.

There are various ways in which a project can impact on privacy or can introduce a risk to privacy. Privacy risks to individuals usually have associated compliance risks and risks to the organisation. For example risk of fines, reputational risk, loss of business and failure of the project.

As part of the PIA we recommend that organisations identify; risks to individual privacy, compliance risks and related corporate or organisational risks. This is because, when deciding how to address privacy risks and assessing the relative costs of each privacy solution, decision makers will usually want to take into account all the risks that arise.

Possible risks include:

Risks to individuals	Compliance risks	Corporate risks
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. 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	Non-compliance with the DPA. Non-compliance with the Privacy and Electronic Communications Regulations (PECR). Non-compliance with sector specific legislation. Non-compliance with human rights legislation.	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.

Risks to individuals	Compliance risks	Corporate risks
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.		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.

Annex three can be used to help organisations identify DPA compliance risks.

There are various approaches to risk management and the PIA process does not require a particular method to be used. Organisations should develop their own ways to identify privacy risks and should incorporate this with their existing risk or project management methodologies. They should build on the earlier work of describing the project and the information flows. This will help organisations to take a thorough and consistent approach.

At this stage organisations should make sure that privacy risks are recorded. An organisation can use the template at Annex two to do this or it can develop its own way to do this, based on its more general approach to managing risk.

It may be useful to use a privacy risk register to describe the risks and assess their likelihood and impact. This can be incorporated into an existing risk register if one exists for the project. Smaller scale projects may have a less formal approach to risk, and this can also be reflected in the privacy risk register.

For further advice on assessing the risks associated with data sharing and the use of anonymised information, organisations can refer to the guidance which the ICO has issued:

- Data sharing code of practice;
- Anonymisation: managing data protection risk code of practice.

Chapter 7 - Identifying privacy solutions

Key points:

- Organisations need to identify possible privacy solutions to address the risks that have been identified.
- A PIA should set out the organisation's options for addressing each risk that has been identified and state whether each option would result in the risk being:
  - eliminated,
  - reduced, or
  - accepted.
- The likely costs and benefits of each option or solution should be evaluated.
- Organisations may wish to use their existing project management or risk management methodologies to help them identify and evaluate privacy solutions.
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to decide how address risks associated with the use of anonymised personal data
- The ICO's Data sharing code of practice may help organisations to decide how to address risks associated with sharing personal data with other organisations.

At this stage organisations should identify what action could be taken to address risks to privacy. Again, this will depend on the nature of the project. The assessment should include an appropriate level of consultation but the whole project does not necessarily need to stop while this step is completed.

When an organisation is deciding on privacy solutions it needs to consider whether the impact on privacy is proportionate to the aims of the project. Privacy solutions are steps which can be taken to reduce the privacy impact. The aim of this stage of the process is to balance the project's outcomes with the impact on individuals.

Organisations can identify and develop possible privacy solutions as part of their normal project management process or by using their preferred risk management methodology. This means that this stage of the PIA might take place at the same time as other aspects of the overall project are developed.

It is important to remember that the aim of a PIA is not to completely eliminate the impact on privacy. Any process which involves the use of personal data will have an impact on privacy and will require a level of risk. Organisations should maintain a focus on ensuring that any impact on privacy is proportionate and there is a necessary and legitimate basis. The purpose of the PIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented. Organisations should record whether each privacy solution that has been identified results in the privacy risks being eliminated, reduced or simply accepted.

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 which 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.

Other costs might include the possibility that collecting less data for privacy reasons will mean having less useful information for a project to use. The aim of the PIA is not to eliminate privacy risks to the extent that the project no longer has any value. Instead organisations should think about how risks can be reduced while still meeting their overall aims. For example, they might be able to retain data in an anonymised format.

At this stage organisations should also assess the extent to which the privacy solutions that have been identified will address the associated compliance risks and corporate risks.

Before implementing a project organisations will need to ensure that it is compliant with the DPA and other relevant legislation. In a DPA context this will include:

- Confirming that the organisation is complying with the data protection principles.
- Identifying the relevant conditions for processing personal data.
- Ensuring that the organisation’s entry on the register of data controllers is still accurate.

Assessing the extent to which each possible solution addresses privacy, compliance and associated corporate risk, and providing a cost benefit analysis of each solution, will assist in the next stage of the PIA. It will help the person responsible for signing off the PIA and deciding which privacy solutions to implement if they have as full a picture as possible.

The template at Annex two can be used to record the key findings of this stage of the PIA. Alternatively organisations can use their existing project management paperwork.

Chapter 8 – signing off and recording the PIA outcomes

Key points:

- A key part of the PIA process is deciding which privacy solutions to take forward and recording whether the risks that have been identified are to be eliminated, reduced or accepted.
- Sometimes organisations will decide that an identified risk is acceptable. However, if there are unacceptable privacy risks which cannot be eliminated or reduced then the organisation will need to reassess the viability of its project.
- It is good practice to record details of the decision maker who has signed off each risk and the reasons behind their decision.
- Publishing a PIA report will improve transparency and accountability and help individuals understand how a project affects them.

Conducting a PIA is primarily about the process of identifying and reducing risks. Those are the stages which will provide assurances that you are using information in a way which is appropriate for your objectives and safer for individuals. However, it is also important to keep a record of the process. This will ensure that the necessary measures are implemented. It can also be used to assure the public, the ICO, and other stakeholders that the project has been thoroughly assessed.

The template provided at Annex two can be used to record the outcomes of the PIA process. Alternatively organisations may choose to use their existing project management paperwork.

Privacy risks register should be updated to reflect how these measures have changed the level of risk. When an organisation accepts risks it should explain why it has decided to do so. The register should record each risk, explain what action has been taken or will be taken and identify who is responsible for approving and implementing the solution.

There is no requirement to produce a PIA report but it will be good practice to do so. If the template at Annex two has been completed as the PIA progresses then this can act as the final PIA report. Otherwise a report should be completed towards the end of the process, drawing on any relevant project management paperwork to summarise the steps that have been taken.

The report can include or reference the material which was produced during the PIA, for example the description of data flows and the privacy risk register. The report should include an overview of the project, explaining why it was undertaken and how it will impact on privacy. It should also describe how the privacy risks were identified and how they will be addressed.

A PIA does not necessarily require a formal signing-off process, but this will depend on the nature of the project. If you are working on large-scale project with a higher level of risk, it would be good practice to ensure that the PIA has been approved at a senior level. For smaller projects, it can be appropriate for the project leader to accept the privacy risks. A signing-off can also help to ensure that the necessary actions are followed up.

The ICO does not take a role in approving or signing-off PIAs. We have developed this process to focus on self-assessment, and every PIA relies on an organisation's understanding of its own practices. If the ICO is involved in the PIA process, it is more likely to be as a stakeholder during the process of identifying risks and mitigating steps.

Publishing PIA reports

The ICO encourages all organisations to publish material relating to a PIA, including the PIA report if one has been produced. Publication improves transparency and can increase the public's understanding of a how their information is used.

A PIA report may sometimes contain information which it is not appropriate to disclose, such as information on security measures. It is good practice for an organisation to disclose as much of the report as it can and only redact the most sensitive elements.

A PIA report may not be the only document which is produced as a result of the assessment. For example, the PIA might identify the need for a new privacy notice for individuals. These other publications can be just as important to make available.

It is recommended practice for public authorities covered by the Freedom of Information Act (FOIA) to include PIA reports in their publication scheme under section 19 of FOIA. The guidance is set out in the definition documents for each sector.

Chapter 9 – Integrating PIA outcomes back in to the project plan

Key points:

- Organisations will need to make sure that the agreed privacy solutions are integrated back into the project plan to be developed and implemented.
- Organisations can use their usual project management methodology to deliver the privacy solutions.

The results of the PIA should be fed back into the wider project management process. This will usually need to take place while the project is still being developed.

Most of the work required by a PIA will take place during the planning and early implementation of a project. However organisations should also take care to ensure that the steps taken as a result of the PIA have been properly implemented and are having the desired effect.

If the project aims develop or change during the project lifecycle you may need to revisit your screening questions to ensure your PIA is still appropriate. This might be especially important with particular project management methodologies which may not have a fixed set of requirements at the outset.

As with other aspects of the PIA process, a review of the privacy outcomes can be built into existing procedures. If an organisation would review the general implementation of a new project after a certain period, it should be possible to include a process for checking the work arising from the PIA as well. The PIA process should be developed to integrate with an organisation’s own project management processes and most project management methodologies include a post project review.

Further reading

There are several sources of further information about PIAs. These may be of particular interest to people wanting to learn more about the different approaches used internationally.

- Privacy impact assessment and risk management – report produced for the ICO by Trilateral Consulting

- *The Privacy Impact Assessment Framework for RFID Applications*, Brussels, January 2011. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

- Art. 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Brussels, Adopted on 11 February 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

- Commission Nationale de l'Informatique et des Libertés (CNIL), *Methodology for Privacy Risk Management*, Translation of June 2012 edition, Paris, 2012. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

- Commission Nationale de l'Informatique et des Libertés (CNIL), *Measures for the privacy risk treatment*, Translation of June 2012 edition, Paris, 2012. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf

- Her Majesty Treasury, *The Orange Book: Management of Risk - Principles and Concepts*, London, October 2004. http://www.hm-treasury.gov.uk/d/orange_book.pdf

- PIAw@tch. http://www.piawatch.eu/

- Ministry of Justice guidance on PIAs http://www.justice.gov.uk/downloads/information-access-rights/data-protection-act/pia-guidance-08-10.pdf

- New Zealand Office of the Privacy Commissioner PIA handbook http://www.privacy.org.nz/news-and-publications/guidance-notes/privacy-impact-assessment-handbook/

Annex one

Privacy impact assessment screening questions

These questions are intended to help organisations 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.

You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

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?

Annex two

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process which is used in this code of practice. You can adapt the process and this template to produce something which allows your organisation to conduct effective PIAs integrated with your project management processes.

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

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 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.

Step three: identify the 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.

Annex three can be used to help identify the DPA related compliance risks

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: 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:** is the risk eliminated, reduced, or accepted?

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 which may arise in the future?

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

Contact point for future privacy concerns

Annex three

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 DPA or other relevant legislation, for example the Human Rights Act.

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?

Annex four

Integrating PIAs with project and risk management

The PIA process is most effective if it is closely integrated with an organisation’s existing project management processes. This helps to ensure that the PIA is able to influence the development of a project. It also encourages all people in a project team to think about privacy risks.

Organisations carrying out PIAs should think about how they can integrate the key principles in this guidance with their existing project management process. The ICO encourages organisations to develop their own templates, screening questions and consultation methods if this is the best way for them to conduct a PIA.

Project management processes are often adapted and become unique to an organisation and it is not possible for this guidance to cover every possible aspect of the numerous different project management processes in use in this context. This annex suggests how PIAs could be integrated with some of the more popular or influential project management methodologies. Organisations that are interested in a more detailed analysis of how PIAs fit together with project management and risk management methodologies and may wish to read the research project report Privacy impact assessment and risk management prepared for the ICO by Trilateral Research and Consulting.

At the most basic level, and whichever methodology an organisation uses, it should adapt the process to include a mechanism which prompts it to identify the need for a PIA. Once the need for a PIA has been identified then using this Code and the template at Annex two should prompt the organisation to consider everything it needs to and to ensure that the PIA findings feed back into the project and influence the final outcomes.

Beyond that, organisations may wish to consider how to match stages of their existing project management process to stages of the PIA process.

The examples in this annex focus on the methodologies which are most well known, or are used in areas where the use of information is more likely to impact on people’s privacy.

Mapping project and risk management concepts onto the PIA process

Step 1 -Identifying the need for a PIA

<u>PRINCE2</u>
The stage of 'Staring up a project' is aimed at ensuring that all the prerequisite elements for initiating the project are in place. This could be adapted to include ensuring that the need for a PIA is identified as a prerequisite element when appropriate.

<u>Agile projects</u>
Most Agile methodologies include an element of meeting user needs. These could include the privacy needs of those affected by the project.

<u>Project management body of knowledge (PMBOK)</u>
Specific goals for privacy could be introduced at an early stage in the scope management knowledge area. This can ensure that all project teams consider whether a PIA is necessary.

Step 2 - Describing information flows

Understanding how you plan to use information is an important aspect of the PIA process. It will allow you to work systematically through the potential risk areas.

<u>PRINCE2</u>
Describe the data flows during the project initiation phase. A full understanding of how the project will work in practice will help you to assess its value against the business case by allowing you to manage risk and remove unnecessary processes.

<u>Agile projects</u>
Describe the information flows as part of a user story which you can refer to while implementing the project. As the project progresses, record how each stage has changed how you use personal information.

Step 3 - Identifying risks

As this aspect of the PIA process concerns risk identification it is particularly likely to be enhanced by using a specific risk management methodology.

<u>PRINCE2</u>

Ensure that privacy risks are included in your organisation’s general approach to risk. Develop standards which all projects should be expected to meet. The ‘identify’ element of the PRINCE2 risk management strategy and procedure (identify-assess-plan-improve) can equate to this stage of the PIA.

Agile projects
Devise ways to quickly check against standard privacy risks during each cycle. Listen to user feedback to understand how privacy risks are arising from the project’s implementation.

ISO31000
An organisation which follows the ISO31000 standard will have developed processes for identifying and recording risks. The PIA process can be integrated at this stage, so that privacy risks are measured in line with corporate standards.

PMBOK
Privacy risks should be included as part of the project risk management area. An organisation’s risk management processes can be used to contribute to the PIA.

Step 4 - Identifying privacy solutions

PRINCE 2
The assess element of the PRINCE2 risk management strategy and procedure (identify-assess-plan-improve) can equate to this stage of the PIA.

Agile projects
If issues are identified, make it a requirement of the next cycle that privacy solutions are implemented.

Step 5 - Signing off and recording the PIA outcomes

PRINCE2

The signing off of the outcomes of a PIA has similarities to managing a stage boundary using PRINCE2. In PRINCE2 the process is completed at the end of a stage, when the project manager reports to the project board sufficient information to enable an assessment of the stage and allow for continuation on to the next stage. In a PIA signing off the outcomes allows the choice of solution to be taken forward for development and implementation.

Agile projects

Signing off a PIA which sets out the privacy solution that needs to be implemented can be seen as setting a requirement. A principle of Agile software development is to welcome changing requirements.

Step 6 - Integrating the PIA outcomes back into the project plan

PRINCE2

Controlling a stage within PRINCE2 includes assigning work and responsibility for actions to ensure that the project proceeds.

Agile projects

A principle of Agile software development is that at regular intervals the team reflects on how to become more effective, then tunes and adjusts its behaviour accordingly. The team should look at lessons learned about privacy risks, and build this into their ongoing work.

PMBOK

As part of the project integration area, an organisation should look closely at ensuring that the PIA outcomes are fully implemented.

Key methodologies and PIAs

PRINCE2

Business case
A business case developed for a project can be an ideal base for a PIA. The business case should set out the project proposal and explain how the project will benefit the organisation. Privacy standards could be established as requirements that must be achieved in all projects.

Engaging stakeholders
When identifying project stakeholders use the opportunity to identify who needs to be engaged to consider privacy issues and how you will work with them. In particular, work to identify stakeholders who can represent the views of individuals affected by the project.

Learning from experience
If possible, review how privacy has been approached on other similar projects. This can include various aspects of the project, from security protocols to media handling. Record information about your PIAs in a way which will allow the organisation to find them useful for future projects.

Risk management
Develop an approach to PIA which balances privacy risks against the objectives of the organisation. Use your existing risk management approach to help you to consistently evaluate privacy issues.

AGILE

The variety of Agile project management systems means that it is more difficult to provide general guidance. The nature of Agile projects means that privacy issues are not always considered using a systematic approach. There is the potential for organisations to incorporate the principles of PIA into their Agile projects.

Smaller PIA tasks
Develop ways to identify and address privacy issues as part of specific work tasks. Agile projects are likely to have less of a focus on a final PIA report but can still undertake other PIA tasks during the project. For example, user testing could include taking feedback on privacy concerns.

Organisation standards for privacy
Establish organisational standards for privacy which all projects can be compared against. These should be practical measures which you can use to check that a project is meeting the required standard.

Feeding back privacy issues
Allow your projects to be shaped by reacting to privacy concerns and be prepared to revisit changes to projects which are found to cause problems.

ISO31000

Consultation
Seek the views of different groups when you are defining risk criteria. This should include taking individuals' expectations of privacy into account.

Accountability
Use the PIA process to identify who in the organisation will be responsible for managing the identified risks.

The Orange book: management of risk

Compliance with data protection requirements is a potential legal risk for organisations to consider as part of their risk assessment. PIA activities can be applied so that they contribute to the understanding of risk in this context.

Privacy risks can be addressed using the same approach as the wider project risks. The concept of proportionality can be useful in this approach. The PIA is not seeking to eliminate risks but is ensuring that the level of risk is appropriate for the nature of the project.

PIA should be seen as something which can improve transparency and public understanding. In turn, this can reduce the risks associated with reputational damage, and the failure of a project to deliver its objectives because of how it is viewed by the public.

Other methodologies

The Trilateral report provides a more detailed overview of the following methodologies:

PMBOK
PRINCE2
Agile
HERMES
ISO31000:2009 Risk management – Principles and guidelines
Combined code and Turnbull guidance
UK Treasury's Orange Book: Management of risk
ENISA's approach to risk management
ISO/IEC 27005:2011 Information risk security management
IT-Grundschutz
NIST SP 800-39 Managing information security risk
ISACA and COBIT
CRAMM
EBIOS
OCTAVE
NIST SP 800-30 Guide for conducting risk assessments
ISO/IEC 29100:2011 Information technology – Security techniques
NIST SP 800-122 Guide to protecting the confidentiality of PII
CNIL methodology for privacy risk management