

Privacy Impact Assessment – an overview

Privacy Impact Assessment

What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions.

Who is required to complete a PIA?

There is no statutory requirement for any organisation to complete a PIA. However, central government departments have been instructed to complete PIAs by Cabinet Office. The ICO has produced the PIA handbook to help organisations assess privacy risks and liabilities.

Why should I do a PIA?

- To identify privacy risks to individuals.
- To identify privacy and DP compliance liabilities for your organisation.
- To protect your reputation.
- To instil public trust and confidence in your project/product.
- To avoid expensive, inadequate “bolt-on” solutions.
- To inform your communications strategy.
- Enlightened self-interest.

When should I start a PIA?

PIAs are most effective when they are started at an early stage of a project, when:

- the project is being designed;
- you know what you want to do;
- you know how you want to do it; and
- you know who else is involved.

But ideally it should be started before:

- decisions are set in stone;
- you have procured systems;
- you have signed contracts/ MOUs/agreements; and
- while you can still change your mind!

Key elements of a PIA

The ICO PIA handbook

This helps you to conduct a PIA and is available at www.ico.gov.uk. It contains advice on the following key features of a PIA.

Initial assessment

Examines the project at an early stage, identifies stakeholders, makes an initial assessment of privacy risk and decides which level of assessment is necessary.

Full-scale PIA

Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.

Small-scale PIA

Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project

Privacy law compliance check

Focuses on compliance with various “privacy” laws such as Human Rights Act, Regulation of Investigatory Powers Act and Privacy and Electronic Communications Regulations as well as the Data Protection Act. Examines compliance with statutory powers, duties and prohibitions in relation to use and disclosure of personal information.

Data protection compliance check

Checklist for compliance with DPA. Usually completed when the project is more fully formed.

Review and redo!

Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should be subject to a PIA.

Top tips for conducting a Privacy Impact Assessment

Do I have to do a PIA for every project?

Not every project will require a PIA. The ICO envisages PIAs being used only where a project is of such a wide scope, or will use personal information of such a nature, that there would be genuine risks to the privacy of the individual. PIAs will usually be recommended where a change of the law will be required, new and intrusive technology is being used, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way. The screening questions in the ICO PIA handbook should provide a good guide as to which level of PIA, if any, is recommended.

Completing an initial assessment

Make sure you use an up to date version of documents such as the terms of reference or the project initiation document. Create a team to oversee and conduct the PIA which represents the project team and privacy professionals within your organisation. Start to list the people, groups and organisations that might have a stake in the project, or be affected by it. The screening questions from the ICO PIA handbook should be completed by the PIA team to see which level of PIA is required.

Completing a full-scale PIA

See which of the stakeholders are best placed to provide effective feedback and decide on your list of consultees. Hold some preliminary discussions with key stakeholders if this helps. Remember that this consultation can be completed alongside other forms of consultation. Use what works best for you – focus groups, open meetings or written consultations. Ensure that you complete your own, internal privacy risk analysis while the consultation is going on. Compare consultation responses with your own internal analysis and identify the privacy problems and solutions. Set out action points and a date when they will be revisited and reviewed.

Completing a small-scale PIA

Remember this does not have to be as formalised or resource intensive as a full-scale PIA and can be scaled up or down to suit the project being assessed. Think of how best to gather opinions of stakeholders – can this be done in a meeting, with a letter or during a phone call? How will you record their views and feed them into your own analysis?

Legal compliance checks and data protection compliance checks

Remember that you do not need to have conducted a PIA in order to check that your project is compliant with the Data Protection Act 1998 and other legal requirements.

Review and redo!

Once you have set a date for reviewing the action points, make sure it goes in everyone's calendar!

www.ico.gov.uk