Australian Government
Office of the Australian Information Commissioner

10 steps to undertaking a privacy impact assessment

When developing or reviewing a project, consider the need for a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy and makes recommendations to manage, minimise or eliminate privacy impacts.

We recommend that organisations conduct PIAs as part of their risk management and planning processes. While each project is different, a PIA should generally include the following 10 steps.

1. Threshold assessment

Ask if any personal information will be collected, stored, used or disclosed in the project. If the answer is yes, a PIA is usually necessary. Keep a record of this threshold assessment.

2. Plan the PIA

Consider the scope of your assessment, who will conduct it, the timeframe, budget and who will be consulted.

3. Describe the project

Prepare a project description to provide context for the PIA project. This should be brief, but sufficiently detailed to allow external stakeholders to understand the project.

4. Identify and consult with stakeholders

Identify the project stakeholders. Consulting them can help to identify new privacy risks and concerns, better understand known risks, and develop strategies to mitigate all risks.

5. Map information flows

Describe and map the project's personal information flows. Detail what information will be collected, used and disclosed, how it will be held and protected, and who will have access.

6. Privacy impact analysis and compliance check

Critically analyse how the project impacts on privacy. Consider compliance with privacy legislation and any other information handling obligations that may apply to your organisation. Even if the project appears to be compliant with privacy legislation, there may be other privacy considerations that need to be addressed such as community expectations.

7. Privacy management — considering risks

Consider options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis.

8. Recommendations

Make recommendations to remove, minimise or mitigate the risks identified through the privacy impact analysis. Include a timeframe for implementing the recommendations.

9. Report

Prepare a report that sets out all the PIA information. It should be a practical document that can easily be interpreted and applied. The OAIC encourages the publication of PIA reports and has developed a PIA tool to help you conduct a PIA, report its findings and respond to recommendations.

10. Respond and review

Monitor the implementation of the PIA recommendations. A PIA should be regarded as an ongoing process that does not end with preparation of a report. It is important that action is taken to respond to the recommendations in the report, and to review and update the PIA, particularly if issues arise during implementation.

See our Guide to undertaking privacy impact assessments, e-learning course and PIA tool for more information.

OAIC