office of the privacy commissioner
new south wales

Fact Sheet
December 2016

FS2016/001

Privacy Impact Assessments: An Overview

This resource provides a general description on how to conduct a Privacy Impact Assessment (PIA). For more information and tips on how to conduct a PIA, please refer to our PIA Guide.

Why undertake a PIA?

A Privacy Impact Assessment (PIA) allows you to identify and address privacy risks associated with your project before it is too late.

A PIA is more than achieving regulatory compliance - it enhances the quality of information before decision makers and demonstrates that a project has been designed with privacy in mind.

When to undertake a PIA?

The timing of a PIA is crucial. A PIA should be conducted early enough so that it can genuinely affect project design, yet not too early as to prevent you from obtaining the necessary information about the project to adequately assess any privacy risks.

What are the core elements of a PIA?

The *PIA Guide* describes seven key elements to achieve an effective PIA. A PIA should be:

- ***Integral*:** the PIA should be integrated into your organisation's governance structure and have clear guidance on who has responsibility over the PIA;
- ***Fit for purpose*:** the PIA should be commensurate with the potential privacy risks associated with the project;
- ***Comprehensive*:** the PIA should cover all privacy issues, not just information privacy. A PIA should also consider whether change is required in supporting documentation such as Privacy Management Plans, human resource policies or training material to accompany project implementation;
- ***Available*:** the PIA report should be publicly accessible. Where this is not possible, consider releasing a PIA summary report to notify and seek feedback on privacy issues;
- ***Enables compliance*:** the PIA must address all privacy obligations, including the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) where relevant;
- ***Ongoing*:** the PIA should contain an ongoing review mechanism to assess privacy issues throughout the life cycle of the project; and
- ***Constructive*:** the PIA should support your organisation's privacy culture and reference your organisation's risk management process.

What is the PIA process?

The *PIA Guide* provides a twelve step process for creating an effective PIA. These steps may overlap or be revisited, depending on the project's nature and complexity.

1. Determine whether a PIA is necessary

A threshold assessment helps determine whether a PIA is necessary, and if so, the scale and scope of the PIA.

Factors that may determine whether a PIA is necessary include the type of privacy risks involved (e.g. does it involve personal or health information), the context of the project, the size and complexity of the project, any cross-jurisdictional information sharing arrangements that are in place or technological risks.

2. Project planning

If a PIA is necessary, next assign the roles and responsibilities of team members, the terms of reference and allocation of resources (including time) for the PIA. Start identifying key stakeholders who have a privacy interest in the project and initiate ongoing consultation.

3. Undertake the assessment

To undertake the assessment, start by mapping the information flows and identifying any privacy risks throughout the lifecycle of the project. Each information event, including collection, use, disclosure or destruction of information may raise specific privacy issues.

4. Consult with stakeholders

Stakeholders should be provided with sufficient information and time to identify the privacy impacts associated with a project. The views of stakeholders should be considered at a time which allows feedback to shape the project's design.

5. Check for compliance

The PIA should address obligations under the PPIP Act and HRIP Act, including the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs). The PIA should also address compliance against any relevant Public Interest Directions, Codes of Practice or other privacy legislation, if applicable.

6. Identify risks and possible solutions

The PIA should not only consider the content of the information handled by the project, but also its context. For instance, sensitive information may present significant privacy impacts if mishandled.

Potential solutions may include management and operational controls (e.g. amending agency policies or procedures), technical controls (e.g. encryption methods or design changes) or physical controls (e.g. limiting access to certain areas).

7. Formulate and consult on draft recommendations

The draft recommendations may consider that the project should not go ahead, that changes to the project should occur, further consultation is required or that the project does not present any privacy risks in its current form. Your draft recommendations may also consider that amendments to your organisation's Privacy Management Plans or other privacy documentation are required.

The draft recommendations should receive initial approval (including approval from an Audit and Risk Committee where necessary) to determine whether significant action for the project under Step 9 – Implementation is required.

8. Prepare and publish the report

A draft PIA report generally includes a background description, project description, PIA methodology, description of information flows, results from consultation, outcome of the risk assessment and compliance checks, recommendations to mitigate any identified risks and a description of any privacy risks that cannot be mitigated (including how these risks are outweighed by the public benefit delivered by the project). The PIA report should also consider if any approach is to be made to the NSW Privacy Commissioner.

9. Implement the endorsed recommendations

The organisation's response to a PIA report should be fed back into project management and project plans. The PIA report or report summary, along with the organisation's response, should be published to improve the transparency of the project.

Endorsed recommendations need to be monitored and reported on during implementation.

10. Audit and review

Third party review can occur once a PIA report is finalised, or earlier during the PIA process. Keeping a PIA register may also be useful to help identify any systemic privacy issues experienced between projects or by the organisation generally.

11. Update the PIA if there are changes in the project

A PIA should be revisited where there are significant changes to a project proposal; for instance differences to how information obtained will be handled.

12. Embed privacy awareness throughout the organisation and ensure accountability

Evaluate your PIA performance and use this information to improve your organisation for future PIA successes.

For more information

Contact the Office of the Privacy Commissioner

PO Box R232, Royal Exchange, NSW 1225

Level 3, 47 Bridge Street, Sydney NSW 2000

Telephone: (02) 8258 0066

Email: privacy@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au/privacy