The independent regulator fostering trust and accountability in WA through privacy and freedom of information.

Guidance for IPP Entities

Introduction to Privacy Impact Assessments

Office of the Information Commissioner
Western Australia

Publication date: 29/10/26

Version Control: 1.0

Introduction to PIAs

Overview

The *Privacy and Responsible Information Sharing Act 2024 (WA)* (PRIS Act) requires Western Australian public sector entities and their contracted service providers (called IPP entities) to undertake a Privacy Impact Assessment (PIA) in certain circumstances.

The purpose of this resource is to help IPP entities understand the objective and benefits of conducting a PIA.

This is the first resource in a suite of three resources designed guide IPP entities through why, whether and how to conduct a PIA:

1. **WHY:** Introduction to PIAs
2. **WHETHER:** Do I need to do a PIA?
3. **HOW:** How to do a PIA

These resources should be read together. They are available on the Office of the Information Commissioner Western Australia's (OIC WA) website.

What is a PIA?

A PIA is a scalable tool for identifying, assessing and mitigating privacy risks. A PIA assists an IPP entity to identify:

- whether a project involves the handling of personal information
- the privacy risks of the project and whether the project complies with the privacy requirements of the PRIS Act, including the Information Privacy Principles (IPPs), and
- strategies to manage, reduce or eliminate privacy risks.

A PIA can also be used to highlight the positive privacy aspects of a project. For example, a PIA might identify how a project minimises the collection of personal information and how privacy is embedded into the design of the project.

A PIA is usually conducted on a project and is an important step in the project management lifecycle. The term 'project' is used throughout this suite of resources to refer to initiatives undertaken to implement IPP entities' functions and activities. For example, this might include the implementation of new systems or processes, changes to existing systems or processes or the development of new legislation or government policy.

What makes a good PIA?

A good PIA adds value by building privacy into the planning, implementation and ongoing improvement of a project. PIAs can help turn privacy considerations into practical actions and embed good privacy practice in day-to-day decision making.

A good PIA:

- Shapes the design of the function or activity. For new functions or activities, a PIA should be performed whilst there is still time to change things.
- Is not a checkbox activity. PIA findings inform and improve the performance of the project.
- Has a clearly defined scope.
- Considers all potential privacy impacts, with a focus on impacts to the privacy of individuals, not just impacts to the IPP entity.
- Is informed by input from, and is made available to, all relevant stakeholders.
- Is resourced to ensure there is sufficient time and budget to complete the PIA.
- Is an ongoing process. A PIA should be reviewed during project development and after implementation.
- Is not an isolated activity. PIAs should be integrated with existing project management and governance structures.

Why do a PIA?

A PIA supports an IPP entity to embed robust privacy practices into its functions and activities from the outset. This is known as 'privacy by design'. Privacy by design is the most effective method of managing privacy risks. This is because it is more effective to manage privacy risks proactively rather than to make retrospective changes to address issues after they arise.

There are some circumstances where the PRIS Act requires an IPP entity to conduct a PIA. These include:

- before an IPP entity first performs a high privacy impact function or activity
- when an IPP entity makes a significant change to the way in which personal information is handled as part of a high privacy impact function or activity, or
- before entering into an information sharing agreement if the activity is likely to have a significant impact on privacy, involves data integration or data linkage, or any of the proposed recipients is an external entity.

Even where a PIA is not required under the PRIS Act, a PIA can assist an IPP entity to understand its privacy risk exposure and identify how it meets its obligations under the IPPs. A PIA can be particularly valuable to understand privacy risks related to legacy systems or activities that commenced before 1 July 2026 when PRIS became operational.

A PIA can be an effective way for an IPP entity to demonstrate to the public it is actively considering privacy. To this end, making PIAs publicly available helps support Open Government Principles and is an opportunity for an IPP entity to build public trust and confidence in the way it handles personal information. This can, in turn, improve public uptake and increase the likelihood of project success.

When in the project lifecycle to do a PIA?

A PIA undertaken early in the development of a project has the best chance of having a meaningful impact. A PIA should be conducted during the design or planning phase of a project. This allows the privacy impacts to be identified and addressed upfront, before key decisions have already been made.

Identifying privacy impacts early allows IPP entities to consider different design options and implement measures to reduce or eliminate privacy risks before they become embedded. When undertaking a PIA, the IPP entity must remain open to performing the project in a different way to reduce the impact on individuals' privacy, whilst still achieving the intended outcome.

In any case, a PIA should not be done simply to justify decisions that have already been made.

A PIA is not a one-off exercise. This is because projects often evolve as they progress and new privacy risks become evident after implementation. This means PIAs need to be conducted (or reviewed) at multiple stages including:

- during the development stage of the project
- prior to implementation, and
- any time there is a change that could result in new or increased privacy impacts.

Who should conduct a PIA?

There are no prescribed rules about who must conduct a PIA. However, PIAs are usually conducted under the oversight of the IPP entity's privacy officer.

The appropriate approach will depend on a range of factors, including the resources available and the risk profile of the project. PIAs are often overseen by an IPP entity's privacy officer or members of their team. However, a PIA will always require substantial input from the project's business owner.

A PIA is most effective when it incorporates input from a range of stakeholders, including people with privacy expertise and people with a sound understanding of the project's technical and operational design. The project owner also has an important role in considering the findings of the PIA and making decisions in relation to any recommended actions.

When might an IPP entity seek an independent view?

Some projects may benefit from the PIA being conducted by an independent provider. An IPP entity might engage a suitably qualified provider, such as a privacy consultant, legal adviser or other specialist where:

- the project is particularly complex
- the potential privacy impacts are significant
- specialist expertise is not available internally, or
- an independent assessment would help build public confidence in the outcome.

An independent provider can also provide a "second pair of eyes" and identify issues internal project teams may have overlooked.

Next steps?

The next step is to determine whether a PIA is required by undertaking a privacy threshold assessment.

A privacy threshold assessment is a preliminary assessment to help an IPP entity determine whether it should undertake a PIA. The outcome of a privacy threshold assessment will be a recommendation

about whether a PIA should be conducted. It is not a "mini" PIA to determine the level of risk and identify mitigation strategies.

For more information on how to do a privacy threshold assessment see 'Do I need to do a PIA'.

References

Office of the Australian Information Commissioner, *Guide to undertaking privacy impact assessments* (2021) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>

Office of the Information Commissioner Queensland, *Privacy impact assessments* (2025) <https://www.oic.qld.gov.au/government/privacy/privacy-impact-assessments>

Office of the Privacy Commissioner Te Mana Matapono Matatapu, 'How to do a Privacy Impact Assessment' <https://www.privacy.org.nz/responsibilities/privacy-impact-assessments/>

Office of the Victorian Information Commissioner, *Privacy Impact Assessment Guide* (2021) <https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-impact-assessment/>

Privcore, 'What makes a great Privacy Impact Assessment' (2024) <https://www.privcore.com/_files/ugd/440bc4_772f0f06b9cf4f37be5da234458062f2.pdf>

Office of the
Information Commissioner
Western Australia

Address: Albert Facey House, 469 Wellington St, Perth WA 6000, Australia
Website: www.oic.wa.gov.au • **Telephone:** +61 8 6551 7888
Freecall (WA country): 1800 621 244 • **Email:** info@oic.wa.gov.au

The independent regulator fostering trust and accountability in WA through privacy and freedom of information.