

Consultation Draft

Do I need to do a Privacy Impact Assessment?



Office of the
**Information
Commissioner**
Western Australia

Overview

The purpose of this resource is to help IPP entities assess whether they are required to conduct a Privacy Impact Assessment (PIA) under the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act). Where an IPP entity is not required to conduct a PIA, this resource is designed to help the IPP entity consider whether there is another reason for conducting a PIA.

A PIA must be conducted:

- before an IPP entity first performs a high privacy impact function or activity, or
- 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.

A PIA is an integral part of good privacy management practice. A PIA:

- is a vehicle for identifying, assessing and managing privacy risks. Where privacy risks are managed effectively, this can reduce, minimise or eliminate potential for negative privacy impacts on individuals and the community more broadly.
- helps an IPP entity consider how it will meet the privacy requirements of the PRIS Act, including the IPPs, when undertaking a function or activity involving the handling of personal information.
- builds public trust by improving transparency and supporting an IPP entity meet public expectations about how personal information is handled.

Undertaking a privacy threshold assessment will help an IPP entity determine whether a PIA is required for a function or activity.

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 is meeting its obligations under the Information Privacy Principles, particularly in relation to legacy activities that commenced before 1 July 2026.

This guidance should be read in conjunction with the following Office of the Information Commissioner Western Australia (OIC WA) resources: 'Introduction to PIAs' and 'How to do a PIA' (note: these resources are currently not available).

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, therefore, be to determine whether a PIA should be conducted. It is not a “mini” PIA to determine the level of risk and identify mitigation strategies.

A privacy threshold assessment does not need to be in a particular form. However, the OIC WA has developed a template to assist IPP entities undertake a privacy threshold assessment. The use of the template is not mandatory

When is a PIA required to be conducted?

A PIA must be conducted:

- before an IPP entity first performs a high privacy impact function or activity, or
- 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, an IPP entity may also choose to conduct a PIA to understand its privacy risk exposure and identify how it is meeting its obligations under the IPPs. This is particularly important in relation to legacy activities where the privacy risks have not previously been formally assessed. For more information about how the PRIS Act applies to activities that commenced before 1 July 2026, please see the OIC WA guidance for IPP entities: [Personal information collected before and after 1 July 2026](#).

What is a “significant change” in the way in which personal information is handled?

The term “significant change” is not defined in the PRIS Act.

A change to the way personal information is handled includes changes to how it is collected, held, managed, used, disclosed, destroyed or de-identified as part of an existing function or activity.

A change to the way personal information is handled will be significant where the change gives rise to new privacy impacts that should now be evaluated or increases the risk of previously identified privacy impacts.

There will be no significant change where the nature, scope, context and purpose of the handling of personal information as part of the function or activity have not changed and the privacy risks remain unchanged.

Example – Significant change

The Department collects personal information about people who access a public health service. The Department has historically securely destroyed the records containing personal information in line with their retention and disposal authority. The Department proposes to de-identify the records containing personal information instead of destroying them so that researchers can examine patterns in service use and identify gaps in access to public health services.

This would be a significant change as there will be a change to the way personal information is handled when it is no longer required for the purpose for which it was collected. The process of de-identification will introduce new privacy risks that will need to be assessed and managed. The Department will also need to identify and manage their obligations in relation to the handling of de-identified information.

Example – No significant change

The Department uses an online learning management system for one of its services. The online learning management system holds the name, contact details, job title and learning records of users. The Department decides to install a routine vendor software update. The update improves the system performance and fixes several system bugs.

This is not a significant change to the handling of personal information, as the type of personal information held in the online learning management system, as well as the way it is used and disclosed, will remain the same and the update will not introduce any new privacy risks.

Information sharing agreements

Under Part 3 of the PRIS Act, a PIA is also required to be conducted before entering an information sharing agreement where:

- the activity under the agreement is likely to have a 'significant impact on the privacy of an individual'
- the activity under the agreement involves data integration or data linkage, or
- any of the proposed recipients is an external entity (section 176).

Further guidance on what is a 'significant impact on the privacy of an individual' and 'data integration and data linkage' is set out below.

The Chief Data Officer has also issued guidelines to support responsible information sharing, including guidance about what assessments must be conducted before entering into information sharing agreements: see [Chief Data Officer Guideline: Assessments for data sharing under the PRIS Act](#).

What is a high privacy impact function or activity?

Section 79 of the PRIS Act provides:

(1) A function or activity of an IPP entity is a high privacy impact function or activity if the performance of the function or activity —

(a) involves the handling of personal information; and

(b) is likely to have a significant impact on the privacy of individuals.

What is “handling personal information”?

A PIA is only required when the function or activity involves the handling of personal information.

Personal information is information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion. For more information see [“What is personal information?”](#).

Personal information is “handled” when any step of the information lifecycle is undertaken. It includes collecting, holding, managing, using, disclosing or destroying personal information.

What is “likely to have a significant impact on the privacy of individuals”?

What does “significant impact” mean?

“Significant impact” is not defined in the PRIS Act. A significant impact on privacy is one that warrants further consideration to identify measures to prevent or mitigate that impact.

A function or activity can still have a significant impact on the privacy of individuals even when a law requires or authorises the handling of personal information, or where an IPP entity relies on another exception to the IPPs.

Whether an activity or function is likely to have a significant impact on privacy, and hence whether a PIA is required, is generally by the potential impact. It is generally *not* assessed based on the residual risk after mitigation strategies have been implemented.

An IPP entity should not assume a function or activity will have no privacy impact where de-identified information is being used. Where a function or activity involves the handling of de-identified information an IPP entity should consider the risks if the information were to be re-identified. This is particularly important where a project involves a data sharing agreement under Part 3 of the PRIS Act or data linkage or data integration.

Whether a function or activity will have a significant impact on the privacy of individuals will depend on the circumstances. Sometimes a single factor may be enough to indicate a PIA should be performed and other times multiple factors together indicate a likelihood of significant privacy impact.

Examples of factors that may indicate a significant impact on the privacy of individuals include:

The function or activity involves:	Potential impact/s:
Personal information handled on a large scale	Large-scale handling may affect many individuals or involve substantial volumes or types of personal information. This can increase both the likelihood of a privacy risk being realised and the scale of the impact.
Sensitive personal information	Sensitive personal information can be associated with discrimination and intrusive collection practices. Some sensitive personal information, such as biometric information, is not easy to change once compromised.
Personal information of children or vulnerable individuals	Some individuals may be more susceptible to harm or face greater difficulty understanding, exercising or protecting their privacy rights.
Personal information of individuals handled without their knowledge	Individuals may be unable to make choices or exercise their privacy rights. The handling may also be unexpected or inconsistent with individuals' expectations.
Tracking individuals or surveillance	Tracking and surveillance may reveal detailed patterns about an individual's movements, behaviour, activities or associations over time. Tracking and surveillance can enable monitoring or profiling of individuals which can increase privacy risks.
Inferred personal information	Inferences may reveal new or sensitive personal information that individuals did not directly provide or expect to be derived. Inferences may be inaccurate but still relied on in ways that affect individuals.
Data linkage or data integration	Combining information from different sources may create a more detailed picture of an individual than any single source. It may also enable new uses of personal information or increase the risk of re-identification of previously de-identified information.
Automated decision-making and artificial intelligence	Automated processes may make or influence decisions that affect individuals quickly and at scale. Errors or bias in automated processes can be replicated widely, and individuals may have difficulty understanding or challenging how a decision was made.
New technology or existing technology used in a novel way	New or novel uses of technology in ways that weren't originally intended may create new privacy risks that are not yet well understood or addressed by established safeguards.
Disclosure of personal information to another entity	Disclosure to a contracted service provider or another third party may reduce the disclosing entity's practical control over how personal information is handled. Depending on the circumstances, including the volume and sensitivity of the personal information involved, this may result in privacy impacts that need to be further considered. Sometimes this may be considered as part of a vendor risk assessment.
Personal information used to make a decision that affects an individual's rights, entitlements, interests or liabilities, or otherwise has a significant effect on an individual's life circumstances, opportunities, behaviour or wellbeing	Personal information used to make decisions of this nature can have serious or lasting consequences for an individual.
Personal information handled in a way that may result in individual harm	Personal harm may include both physical and emotional harm, denial of access to a service, discrimination, financial loss, reputational damage or identity theft.
Personal information handled in a way that may result in collective harm	Privacy impacts may have a collective impact on a particular group of individuals, community or the public more broadly. Collective harm may

occur even when harm to a particular individual is difficult to identify or doesn't appear significant when assessed in isolation. This is because the scale of these impacts may only be evident when viewed across a population or because the impacts accrue gradually over time. Examples of collective harm may include:

- widespread surveillance impacting individual autonomy
- chilling effects, where people self-censor their behaviour or speech
- manipulation of individual behaviour or choice and broader public opinion, and
- profiling resulting in discrimination or marginalisation of particular groups.

What does “likely” mean?

The term “likely” is not defined in the PRIS Act. It should be construed in accordance with the relevant objects of the PRIS Act which includes promoting the responsible handling of personal information. In this context, something is likely to have a significant impact when there is a real chance or possibility that it will occur. This means a significant impact is not likely if it is only a remote possibility.

If an IPP entity is unsure whether a proposed function or activity is likely to have a significant impact on the privacy of individuals, it should conduct a PIA.

Example – Function or activity likely to have a significant impact

A Department proposes to use an AI scribe to maintain a record of meetings staff have with external stakeholders. These meetings are sometimes between staff and members of the public who are accessing public services. The AI scribe summarises the discussion and organises the summary into an approved format. The staff often use the record of meeting minutes when making decisions, including in relation to the provision of services.

The Department has not used AI scribe technology before.

There are several factors indicating this trial may have a significant impact on privacy, including:

- the potential for handling of personal information without the knowledge of the individuals in the meeting or in ways those individuals may not expect
- the use of new technology not previously used by the Department
- potential disclosure of personal information to the third-party provider of the AI scribe technology, and
- the potential for the output of the AI scribe to be used to make decisions, including decisions affecting individuals.

Given the presence of these factors, there is a real or not remote possibility the trial could have a significant impact on privacy, and a PIA should be conducted.

Example – Unclear whether the function or activity is likely to have a significant impact

A Local Government proposes to introduce an online booking system for its community facilities. Residents will be required to provide their name and email address when they make a booking on the system. The Local Government already uses the software provider of the online booking system for other community services.

The Local Government considers the online booking system might create barriers for people who have limited access to, confidence in, or ability to use online services.

The Local Government conducts a Privacy Threshold Assessment but cannot conclusively determine whether the online booking system is likely to have a significant impact on the privacy of individuals. As the Local Government is unsure, they decide to proceed with a PIA so they can consider in detail the privacy impacts of the online booking system and ensure it is implemented consistently with the requirements of the IPPs.

Example – Function or activity unlikely to have a significant impact

A Local Government proposes to introduce an email subscription service for residents who wish to receive updates about upcoming community events. Residents may voluntarily provide their email address through the Local Government's website to receive the emails and can remain anonymous with name being optional. The compiled list of email addresses will only be used for the distribution of the community newsletter and residents will be able to unsubscribe at any time.

The Local Government will continue to provide updates about community events through its existing communication channels, including through social media posts and advertisements in the local newspaper.

The Local Government considers the scale and nature of the personal information handled as part of this activity means it is unlikely the email subscription service will have a significant impact on the privacy of individuals. They document their decision and rationale for not conducting a PIA.

Next steps – how to conduct a PIA

If your privacy threshold assessment recommends that a PIA should be conducted, the OIC WA has published guidance on how to do a PIA as well as a PIA template (note: these resources are currently not available). Use of the PIA template is voluntary.



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.**