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

Guidance for the public

Resource 1: Understanding my privacy rights – when do they commence?

Office of the Information Commissioner
Western Australia

Publication date: 03/03/26
Version Control: 01

Guidance for the public

Resource 1: Understanding my privacy rights – when do they commence?

Does Western Australia have a privacy law?

Yes, the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act) introduces a new privacy regulatory framework which requires the Western Australian public sector to uphold responsible and transparent practices for handling personal information.

The PRIS Act establishes principles that regulated entities need to follow when they collect, use, store, and share your personal information and, in some cases, de-identified information. These are called the Information Privacy Principles (IPPs) (please see our IPP Summary and Full Text IPPs).

The PRIS Act also establishes rights for individuals, including the right to make a complaint to the Office of the Information Commissioner Western Australia (OIC) if you believe a regulated entity has handled your personal information in a way that is inconsistent with the IPPs (called an interference with privacy).

Who must comply with the PRIS Act?

The PRIS Act contains a list of the types of entities required to comply with the Act. These are collectively called 'IPP entities'.

What is an IPP entity?

IPP entities include Western Australian government agencies, departments, statutory authorities, the Police Force of Western Australia, Local Governments, Ministers, Parliamentary Secretaries, government trading enterprises, and some contracted service providers to government.

What rights do I have under the PRIS Act?

From 1 July 2026, the PRIS Act gives you new rights in relation to your personal information in the hands of IPP entities. Once all the privacy provisions in the PRIS Act commence, you will have the right to:

- be informed of how an IPP entity handles your personal information;
- interact with an IPP entity anonymously, unless the law or circumstances require you to identify yourself;
- be notified if an IPP entity uses an automated decision-making process (that is a process without much human input) to make a significant decision about you and request information about that process and human intervention in that decision;
- in some circumstances, access and correct personal information an IPP entity, or their contracted service provider, holds about you;
- make a privacy complaint to the Information Commissioner if you believe an IPP entity has interfered with your privacy; and
- be notified if your personal information was involved in a breach that is likely to cause you serious harm.

When can I exercise my rights under the PRIS Act?

Most of the new rights in the PRIS Act will start on 1 July 2026. The right to be notified if your personal information was involved in a breach that is likely to cause you serious harm starts later, on 1 January 2027.

This means the OIC will be able to receive and investigate your privacy complaints from 1 July 2026. From that date, a privacy complaint must be about an IPP entity handling your personal information inconsistently with the IPPs (i.e. the complaint must be about an alleged interference with your privacy). Importantly, the relevant act or practice you are complaining about must have taken place on or after 1 July 2026. You must also make your complaint to the IPP entity first, before bringing it to the OIC.

Before 1 July 2026, if you are concerned an IPP entity has interfered with your privacy you should make a complaint directly to the IPP entity.

Will the PRIS Act apply to my information if it was collected before 1 July 2026?

Yes, most of the IPPs will apply to your personal information if it was collected before 1 July 2026. However, some IPPs (and the rights they contain) only apply to your personal information if it was collected *on or after* that date.

The following IPPs **do not apply** to personal information collected **before** 1 July 2026:

IPP 1 – Collection

IPP 1 sets out requirements that apply when an IPP entity collects your personal information. For example, an IPP entity must provide you with certain information at or before (or, where that is not practicable, as soon as practicable after) collecting your personal information. This includes information about why it is requesting the information and the consequences if you choose not to provide it (this is called a collection notice).

IPP 1 only applies to information collected *on or after* 1 July 2026. This means, for example, the OIC cannot investigate a complaint about the fact you were not provided with a collection notice if the information was collected before that date.

IPP 7 – Unique identifiers

IPP 7 sets out requirements in relation to the handling of unique identifiers (such as a drivers license number). Under the PRIS Act, unique identifiers are a type of personal information.

IPP 7 applies to the handling of unique identifiers *on or after* 1 July 2026. This means the OIC cannot investigate a complaint about an IPP entity not complying with IPP 7 if the event you are complaining about took place before 1 July 2026.

IPP 8 – Anonymity

IPP 8 provides you with the right to interact with an IPP entity anonymously, unless the law or circumstances require you to identify yourself.

IPP 8 only applies to personal information collected *on or after* 1 July 2026. This means the OIC cannot investigate a complaint about an IPP entity not providing you with an option to engage with them anonymously where the relevant interaction occurred before that date.

IPP 10 – Automated decision-making

IPP 10 requires an IPP entity to take certain steps before using an automated decision-making process (that is a process without much human input) to make significant decisions about you. It also provides

you with certain rights where an IPP entity uses an automated decision-making process to make such decisions.

IPP 10 only applies to personal information collected on or after 1 July 2026. This means the OIC cannot investigate a complaint about the fact an IPP entity used an automated decision-making process to make a decision about you before 1 July 2026.

Example 1 – IPP 1 Collection and IPP 8 Anonymity

A Local Government (the City) has used an online form to collect feedback from residents on the services the City provides (the Survey). The Survey requires residents to provide certain personal information, including their name and email address. The City has been running the Survey annually since October 2021 and the form has never been accompanied by a collection notice.

A resident has completed the online form every year since the City started the Survey in 2021. The resident is concerned about the request to provide personal information, as they would prefer to engage anonymously. Because the obligation to provide a collection notice (IPP 1) and the ability for a person to engage anonymously (IPP 8) only apply to information collected *on or after* 1 July 2026, the OIC cannot investigate a complaint under the PRIS Act about these matters in relation to past surveys.

However, the resident can still contact the City directly in relation to these concerns. If the City does not make the changes necessary to comply with the PRIS Act before running the next Survey in October 2026, the resident may make a complaint to the OIC.

Example 2 – IPP 10 Automated decision-making

A Government agency uses an automated system to review the CVs of applicants for open roles to determine whether the applicant has the experience and skills required by the job description. The agency HR manager responsible for recruitment relies on the automated system's preliminary decision in deciding who to interview.

An individual applied for a job with the agency in December 2025 and subsequently became concerned they were being unfairly discriminated against because of the use of the automated system in the recruitment process. Because IPP 10 (and the obligations it contains) only apply to information collected on or after 1 July 2026, the OIC cannot investigate a complaint from the applicant about the use of the automated system in December 2025.

However, if the applicant were to apply for another job with the agency after 1 July 2026, the agency would be required to notify applicants about the fact that they are using an automated decision-making process and provide them with the option to request human intervention. If the applicant was still dissatisfied with the information the agency provided, they could make a complaint to the OIC provided they have first made a complaint directly to the agency involved.

Notifiable information breaches

The PRIS Act contains requirements that apply where an IPP entity believes or suspects there has been a breach of personal information that is likely to cause you serious harm, called a notifiable information breach. A notifiable information breach might occur because there has been unauthorised access to, or disclosure of, your personal information, or where your personal information was lost in circumstances where unauthorised access or disclosure is likely.

The requirements related to notifiable information breaches apply to all personal information irrespective of whether it was collected before, on or after 1 January 2027. This means the OIC can investigate complaints about an IPP entity's failure to notify you about a notifiable information breach involving your personal information, even if the personal information was collected before 1 January 2027.

Example 3 – Notifiable information breaches

A Government agency holds sensitive medical information about members of the public for the purpose of assessing eligibility for social benefits. This information is held in a database and has been collected over the past 10 years. In December 2027, the agency is the target of a cyber-attack, where a third party was able to gain access to the database and extract the sensitive medical information of over 10,000 individuals.

Even though most of the personal information the breach impacted was collected before 1 January 2027, the Government agency is still required to comply with the notifiable information breach requirements contained in the PRIS Act. In this case, because the breach involved sensitive medical information being accessed by a malicious third party, it is likely that a notifiable information breach has occurred and the agency will be required to notify both the Information Commissioner and affected individuals about the breach as soon as practicable.

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.