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

Guidance for IPP Entities

Resource 1: Personal information collected before and after 1 July 2026

Office of the Information Commissioner
Western Australia

Publication date: 03/03/26

Version Control: 01

Guidance for IPP Entities

Resource 1: Personal information collected before and after 1 July 2026

Overview

The majority of the substantive privacy provisions of the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act) will commence on **1 July 2026**. This will include the Information Privacy Principles (IPPs)[1] which regulate the handling of personal information, and in some cases de-identified information. The IPPs apply to the Western Australian public sector, including contracted service providers. The notifiable information breach provisions contained in Part 2 Division 6 of the PRIS Act, will commence later, on 1 January 2027.

From 1 July 2026 certain obligations (including certain IPPs) will apply to personal information and de-identified information collected before **and** after 1 July 2026. Other obligations will only apply to personal information collected after 1 July 2026.[2]

The purpose of this Resource is to explain how the IPPs and a number of other substantive provisions contained in the PRIS Act apply to personal and de-identified information collected before and after 1 July 2026. This is set out in 'Part 5 – Transitional Provisions' of the PRIS Act. Please read this Resource in conjunction with our IPP Summary and full text IPPs available on the Office of the Information Commissioner Western Australia (OIC) website.

These IPPs apply to personal information collected on or after 1 July 2026

IPP 1 – Collection

IPP 7 – Unique identifiers

IPP 8 – Anonymity

IPP 10 – Automated decision-making

These IPPs apply to personal information collected before, on or after 1 July 2026

IPP 2 – Use and disclosure

IPP 3 – Information quality

IPP 4 – Information security

IPP 5 – Openness and transparency

IPP 6 – Access and correction

IPP 9.1 – Disclosures outside Australia

These IPPs apply to de-identified information collected before, on or after 1 July 2026

IPP 9.2 – Disclosures outside Australia

IPP 11 – De-identified information

Personal information collected before or after 1 July 2026

From 1 July 2026, the following IPPs apply to the handling of personal information irrespective of whether it was collected **before or after** that date.[3]

- IPP 2 – Use and disclosure
- IPP 3 – Information quality
- IPP 4 – Information security
- IPP 5 – Openness and transparency
- IPP 6 – Access and correction
- IPP 9.1 – Disclosure of personal information relating to an individual outside Australia.

Example 1 – IPP 2 Use and disclosure

The Department collected personal information (updated bank details) directly from employees in 2021 for the purpose of paying the employees their wages (the primary purpose). In November 2026, the Department wants to use that personal information for the purpose of performing parallel testing of its new payroll system (the secondary purpose).

As the testing will occur after 1 July 2026, the Department is only permitted to use the personal information for the secondary purpose if the use is 'fair and reasonable' having regard to the matters set out in IPP 2.2 (unless a relevant exception applies).

If the Department determines it is permitted to use the information for the secondary purpose, it must also make a written record of that secondary purpose (IPP 2.4).

Example 2 – IPP 3 Information quality

A Local Government (the City) holds personal information (name, date of birth, residential address and mobile number) for residents who have registered their dog or cat with the City. This information was collected before 1 July 2026. In August 2026, the City wants to use this information to contact local pet owners.

Under IPP 3 the City must take reasonable steps to ensure the contact information it holds is accurate, complete and up-to-date before using that information to contact the pet owners. This obligation applies even though the information was collected before 1 July 2026. This may mean, for example, the City has a process or system to ensure the personal information it holds is updated when a resident notifies them of a change of details.

If the data is old or if the City is concerned about its accuracy, the City may consider contacting registered pet owners with old or expired pet registrations to request them to confirm their contact and pet registration details as part of its PRIS readiness activities.

De-identified information collected before or after 1 July 2026

From 1 July 2026, the IPPs that contain requirements related to the handling of de-identified information will apply irrespective of whether the information was collected **before or after** that date.[4]

- IPP 9.2 – Disclosure of de-identified information relating to an individual outside Australia
- IPP 11 – De-identified information

Example 3 – IPP 11 De-identified information

The Department holds de-identified information it received from Western Australian public universities under a memorandum of understanding in 2024. In November 2026, the Department wants to re-identify the information for the purpose of supporting the development of a new education policy. Under IPP 11, the Department will require written authorisation from the universities to re-identify the information for that purpose before it is permitted to undertake the re-identification.

Personal information collected on or after 1 July 2026

The following IPPs only apply to the handling of personal information collected **on or after** 1 July 2026.[5]

- IPP 1 – Collection
- IPP 7 – Unique identifiers
- IPP 8 – Anonymity
- IPP 10 – Automated decision-making

Example 4 – IPP 1 Collection

A Local Government (the City) uses an online form to collect personal information from ratepayers about changes to property ownership or contact details. Before 1 July 2026, the form did not include the type of information required by IPP 1 (for example a collection notice required under IPP 1.9). Because IPP 1 only applies to personal information collected on or after 1 July 2026, the City is not required to retrospectively provide a collection notice to all ratepayers who completed the online form before that date.

However, if the City continues to use the form after 1 July 2026, it must ensure the form includes a collection notice as required by IPP 1.9 (or ratepayers are otherwise given or made aware of the information set out in IPP 1.9). This includes the purposes for which the City is collecting the information and for which it will be used and disclosed, how the individual can seek access to the information and the main consequences (if any) if they choose not to provide it.

Example 5 – IPP 10 Automated decision-making

Since 2021, the Department has been using an automated system for the purpose of assessing individuals' entitlement to financial rebates.

From 1 July 2026, if the Department wishes to continue using the automated system in relation to rebate applications received after this date it must conduct an assessment of the impact on individuals whose applications are assessed by the tool, having regard to the matters set out in IPP 10.1. This includes consideration of how to eliminate or minimise any harm, bias or discrimination and whether there is a process by which individuals can request human intervention in the decision.

Privacy impact assessments for functions and activities performed before 1 July 2026

From 1 July 2026, IPP entities will be required to conduct a privacy impact assessment (PIAs) before performing, or making a significant change to, high privacy impact functions or activities.[6]

Where an IPP entity commenced the relevant activity **before** 1 July 2026 the entity is not required to retrospectively perform a PIA. However, a PIA must be undertaken:

- if the activity is first performed **on or after** 1 July 2026, even where the activity is performed in connection with a function that the IPP entity started to perform before that date; or
- where the IPP entity makes a significant change **on or after** 1 July 2026 to the way personal information is handled as part of an activity that was commenced before that date.[7]

While the obligation to undertake a PIA does not apply retrospectively, an IPP entity should be aware of what high privacy impact functions or activities it currently performs. A PIA can be a useful tool when considering whether such functions or activities otherwise comply with the requirements of the IPPs.

Example 6 – Privacy impact assessments

In 2025, the Department introduced facial-recognition technology for staff and visitors entering and exiting its premises. Because the activity commenced before 1 July 2026, the Department is not required to retrospectively complete a PIA. However, the Department must conduct a PIA for any significant changes made after 1 July 2026 to the way personal information is handled as part of the facial-recognition system.

While the Department is not required to retrospectively undertake a PIA in relation to the facial-recognition system, undertaking a PIA may help the Department assess whether the system meets the requirements of the IPPs. For example, a PIA might consider whether the collection of facial biometrics is fair and reasonable within the meaning of IPP 1.

Personal information contained in public registers published before 1 July 2026

From 1 July 2026, a public entity responsible for administering a public register must not include personal information in the public register unless it is consistent with the purpose for which the register exists or the law under which it is maintained.[8]

The PRIS Act also provides individuals with a right to request the removal of their personal information from a public register (or not to include their personal information in a public register) on the grounds an individual's safety or wellbeing is or would be substantially affected by the publication of the information.[9]

These provisions apply to personal information irrespective of whether the information was collected before or after 1 July 2026.[10] This means that after 1 July 2026 a public entity must consider the purpose of the register before including any personal information in the register. Similarly, if the public entity receives a request for the removal of personal information included in the public register before 1 July 2026, it must consider that request in line with the provisions of the PRIS Act.

Example 7 – Public registers

In August 2026, a person experiencing family violence requests their personal information be removed from a public register for safety reasons. The public entity responsible for maintaining the register is required to consider the request in accordance with the provisions of the PRIS Act even though the information was included on the register before 1 July 2026.

State services contracts entered into before 1 July 2026

Under the PRIS Act, the IPPs will apply to a contracted service provider (CSP) when performing services under a State services contract provided the contract contains a clause to that effect.[11]

Where a contract was entered into before 1 July 2026, the IPPs will still apply to the services the CSP provides after that date if the contract contains the necessary provision. It does not matter that the relevant obligation to comply with the PRIS Act was included in the contract before 1 July 2026.[12]

Example 8 – Contracted service providers

The Department engages a company to audit the Department's IT systems. The company entered into a State services contract with the Department in December 2025. The contract contains an obligation for the company to comply with the relevant provisions of the PRIS Act when handling personal information for the purpose of providing the services. Even though the contract was entered before 1 July 2026, the IPPs will apply directly to the company's handling of personal information as if it were the relevant Department on and from 1 July 2026.

Notifiable information breaches involving personal information collected before 1 January 2027

On 1 January 2027, the notifiable information breach provisions contained in Part 2 Division 6 of the PRIS Act will commence.

A notifiable information breach may occur in relation to personal information held by an IPP entity irrespective of whether the affected personal information was collected before, on or after 1 January 2027.[13]

Example 9 – Notifiable information breaches

A local government (the City) experiences a cyberattack in February 2027 resulting in unauthorised access to personal information the City holds, including full names, addresses and rates invoices. The personal information was collected before 1 January 2027. Even though the personal information was collected before the notifiable information breach provisions commenced, the City must still comply with the notifiable information breach provisions and may be required to notify the Information Commissioner and affected individuals of the breach.

[1] *Privacy and Responsible Information Sharing Act* (2024) (PRIS Act) Schedule 1.
[2] PRIS Act Part 5.
[3] PRIS Act s 223(3).
[4] PRIS Act s 223(4).
[5] PRIS Act s 223(2).
[6] PRIS Act Part 2 Division 8.
[7] PRIS Act s 227.
[8] PRIS Act s 76.
[9] PRIS Act s 77.
[10] PRIS Act s 226.
[11] PRIS Act s 129.
[12] PRIS Act s 228.
[13] PRIS Act s 225.

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.