Office of the Information Commissioner
Western Australia

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

Privacy & accountability in automated decision-making (ADM)

From 1 July 2026, Information Privacy Principle (IPP) 10 of the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act) introduces new requirements in relation to the use of automated decision-making (ADM) by the Western Australian public sector.

The PRIS Act is the first law in Australia to regulate the handling of personal information in ADM. IPP 10 recognises the importance of improving transparency, mitigating risks and strengthening public trust around the use of artificial intelligence (AI) and other forms of ADM technologies in handling personal information.

What is ADM?

ADM is where a computer system (including an AI system) is used to automate all or part of a decision-making process. ADM can be achieved through simple pre-programmed rules-based systems where decisions are easy to explain, or more complex systems relying on predictive models where the reasons for the decision are opaque and often hard to explain.

An example of rule-based ADM is an automatic online licence renewal process, where the system will issue a renewed licence after checking the relevant fee has been paid and there are no outstanding penalties pending against the licence prior to renewal.

Increasingly, ADM involves the use of AI systems. Compared to rule-based ADM, ADM involving AI systems can process more complexity, often ingesting large amounts of personal information. An example of ADM involving AI is a recruitment system that uses AI to screen CVs and make recommendations about the suitability of candidates.

What are the risks involved when using ADM?

It is important the use of ADM does not erode trust in government service delivery. In particular, the public must have confidence decisions are still being made in accordance with administrative decision-making principles and any risks associated with the use of ADM are identified, assessed and mitigated at the outset.

Below are some examples of recognised risks involved with the use of ADM:

- Algorithmic bias leading to inaccurate, discriminatory or unfair outcomes.
- Coding errors, rule errors or oversimplification leading to legal errors or incorrect decisions.
- Lack of transparency making it hard to understand how a decision was reached and to challenge or seek review of the decision.
- Cybersecurity risks, including vulnerabilities caused by AI agents with hardcoded or excessive permissions to systems storing personal information.
- Exclusion of vulnerable groups from access to public services, such as people with low digital literacy, in financial difficulty or who have access to limited records.
- Over reliance on automated systems leading to the de-skilling of decision makers.

How are automated systems used to assist decision-making?

Under the PRIS Act, ADM includes both where an automated system makes a final decision without human involvement and where an automated system materially assists in making the decision. A decision is considered ‘materially assisted’ if a person makes the decision in reliance on a preliminary step the automated system generates (such as a recommendation, assessment, or inference) and that preliminary step has a material bearing on the decision being made.

Depending on the circumstances, ADM might include where an automated system:

- makes the decision;
- recommends a decision to the decision-maker;
- guides an individual through relevant facts, legislation and policy;
- summarises or makes preliminary assessments for decision makers; and
- automates aspects of the fact-finding process which may influence subsequent decisions, for example by applying data matching.

What does IPP 10 require?

IPP 10 will apply where a WA public sector entity, or their contracted service providers, (called 'IPP entities') employ ADM that:

- involves the use of personal information collected on or after 1 July 2026; and
- is used in making significant decisions about individuals.

A significant decision is one 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.

Where IPP 10 applies to the use of ADM an IPP entity must:

1. Conduct an impact assessment

The IPP entity wishing to use the ADM process must conduct an impact assessment of the ADM process (ADM assessment) that considers:

- how to eliminate or minimise the risk of harm, bias, and discrimination;
- whether there is a process for individuals to request human intervention in decisions made about them; and
- whether the handling of personal information complies with the PRIS Act.

This assessment may be conducted as part of or in conjunction with any other assessments undertaken by the IPP entity, such as a Privacy Impact Assessment or an AI self-assessment. Importantly, the ADM assessment is not a 'set and forget' activity. The IPP entity must periodically evaluate the operation and effectiveness of the ADM process and update the ADM assessment when changes are made to the ADM process.

2. Be transparent

An IPP entity must be transparent about their use of ADM, including by:

- notifying an individual that ADM was used to make a decision about them; and
- on request, providing the individual with sufficient information about how the ADM works in a form they could be reasonably expected to understand.

3. Provide an option for human intervention

An IPP entity must also provide a process for the individual to request human intervention in the decision.

How can IPP entities better manage their use of ADM?

There are several steps IPP entities can take to better manage their use of ADM technologies and the associated risks, including:

- Conducting a stocktake and maintaining a register of ADM processes, either in development or deployed.
- Where ADM is used, completing a self-assessment in accordance with the WA Government AI Assurance Framework to review and manage associated risks.
- Updating the entity's privacy policy and any other relevant communications to clearly state whether any personal information is used in ADM.
- Establishing repeatable processes to monitor the development and use of ADM within the entity's operations to ensure they remain suitable for the intended purpose, manage any incremental expansion in scope and identify any additional risks.
- Ensuring staff using ADM receive training on how automated systems work, any limitations, potential biases, and the circumstances in which human oversight and intervention is required.