

New automated decision-making (ADM) transparency obligation guidance



New OAIC Guidance

On 30 September 2026, the Office of the Australian Information Commissioner (OAIC) released new guidance to support compliance with the ADM transparency obligation introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**POLA Act**) amending the *Privacy Act 1988* (Cth) (**Privacy Act**).

The OAIC has published four separate pieces of material which APP entities can use to inform their compliance:

- a **new version of the APP1 Guidelines**, which includes new paragraphs [1.35]–[1.78];
- **APP 1.7-1.9 Transparency Obligation Fact Sheet**;
- **Supplementary Fact Sheet for government agencies**; and
- **APP 1.7-1.9 Transparency Obligation Flowchart**.

The OAIC has taken a pragmatic approach in their Guidelines. They state:

“APP entities must strike a balance between providing enough meaningful information for individuals to understand their use of a computer program and avoiding excessive detail that obscures the purpose of transparency and clear communication.”

The Guidelines go on to provide a list of factors for organisations to consider in drafting their policies. However, the **most illustrative component of the new material from the OAIC occurs in the Fact Sheet**.

“Example 6” and “Example 7” on the Fact Sheet **provide worked hypothetical examples of automated decision-making use-cases, along with worked examples of what the OAIC considers to be appropriate disclosure** for the purposes of APP1.7.

ADM Transparency Obligation

The ADM transparency obligation is the first in a series of proposed reforms to the Privacy Act to address the risks of evolving technologies such as AI.

The POLA Act adds new sub-clauses to the Australian Privacy Principles (**APPs**) to require organisations to provide transparency into how computer systems are used in decision-making impacting individuals.

APP1.7 defines the scope of the new obligations. If its three sub-clauses are satisfied, the obligation is engaged. Notably:

- any “computer program” (not just AI) is within scope – **tools such as bespoke computer programs, filtering algorithms, or even spreadsheets may be captured** if the criteria are met;
- **outsourcing or contracting a third party does not remove responsibility** for the APP entity – whichever entity has “arranged for” the use of the computer program in the decision is in scope;
- a **“human in the loop” does not displace the obligation** – if the computer program is used to do a thing “substantially and directly related” to the decision; and
- the decision must “significantly affect the rights or interests” of an individual – meaning **there is an opportunity to exclude decisions which do not affect rights or interests of individuals, or which do not significantly affect those rights or interests**.

APP1.8 sets out what information the privacy policy must include. APP entities must document:

- The kinds of personal information used in the operation of computer systems covered by APP1.7;
- The kinds of decisions made solely by the operation of computer systems covered by APP1.7; and
- The kinds of decisions for which a thing, that is “substantially and directly related” to making a decision, is done by the operation of a computer system covered by APP1.7.

APP1.9 provides extra definitions to aid interpretation of APP1.7–APP1.8.

Key Takeaways

The level of detail which organisations must put into an APP1 privacy policy is not particularly onerous once the discovery work is done. The OAIC has helpfully illustrated a compliant approach with clear examples and has given sensible guidance which allows for aggregation of information, provided the aims of APP1 are otherwise met (openness, transparency, clear communication).

The most difficult part of compliance with the new obligation is not the documentation within the privacy policy, but rather the discovery work that informs the policy. Some businesses will have to triage hundreds of different business processes that might use personal information in the course of decision-making to determine whether they are captured by the new obligation.

The requirement to transparently disclose “automated decision-making” in an APP1 privacy policy is broader than AI. It may capture things as routine as low-automation business processes or spreadsheets in some instances. Further, it is likely to extend even to chatbot usage in certain circumstances (whether that use is approved or “shadow” usage).

There is a limited carve-out for “commercial-in-confidence” information. This does not remove the obligation to disclose where a computer system is covered. Instead, it changes the content of the disclosure that is required.

Failure to comply with APP1.7 constitutes an “interference with the privacy of an individual”. Depending on the severity of the interference, this may lead to civil penalties.

Next Steps

Early adopters	Cautious observers	Harnessing opportunity
For APP entities that have already started their compliance journey, an initial analysis of the work done to date will be your guide, and some uplift or adjustment may be required to reach a state of comfort.	For APP entities that have not started action on compliance, prioritise a threshold assessment to identify potentially in-scope activities and inform early drafts of the transparency notice. A concurrent full discovery project can be commenced in parallel to attain compliance.	Beyond bare compliance, projects oriented toward this obligation present a unique opportunity for APP entities to more deeply understand their AI risk profile. A tailored approach can be made for your organisation which collects the information needed for compliance in parallel with information to inform risk and governance discussions around AI going forward.