

APP 1.7-1.9 Transparency Obligation

Supplementary Fact Sheet for Government Agencies

This supplementary fact sheet is intended to help government agencies implement new Australian Privacy Principle (APP) 1 transparency obligations under APP 1.7-1.9, with respect to the usage of computer programs to make or inform decisions (transparency obligation). Changes to privacy obligations for APP entities come into effect on **10 December 2026**.

This supplementary fact sheet does not cover the entirety of an APP entity's privacy obligations and should be read in conjunction with the *Privacy Act 1988* (Cth), Australian Privacy Principles, OAIC's [APP 1 Guidelines](#), OAIC's APP 1.7-1.9 Transparency Obligation Fact Sheet and other OAIC resources referred to in this fact sheet.

APP entities in doubt of whether their use of a computer program falls within the scope of the transparency obligation should take a cautious approach and include information in their APP privacy policy necessary to comply with APP 1.8 requirements.

How does the transparency obligation align with the Freedom of Information Act?

All Government agencies that are subject to the *Freedom of Information Act 1982* (Cth) (FOI Act) are required to comply with obligations of disclosure under the Information Publication Scheme (IPS). That obligation extends to publishing a plan showing how an agency will comply with the IPS and as well as information that sets out what the agency does, the way it does it, and operational information.

Section 8A of the FOI Act defines operational information to include “information held by the agency to assist the agency to perform or exercise the agency's functions or powers in making decisions or recommendations affecting members of the public”.

The Guidelines issued under section 93A of the FOI Act that agencies must have regard to when exercising a function or power make clear that automated decision making (ADM) information should be published, including the types of ADM used and the kinds of decisions ADM is used for, on their websites to satisfy their IPS obligations. Further information is available in [Part 13: Information Publication Scheme](#), and OAIC guidance '[About the Information Publication Scheme](#)'.

The transparency requirements on computer programs under APP 1.7-1.9 further guarantee an individual's knowledge of the circumstances in which their personal information is being used in the context of ADM. Transparency of use broadly underpins this obligation and has a direct relationship to the transparency obligations under the FOI Act in a Commonwealth government context.

All Government agencies authorised under legislative statutes to use ADM should publish this information as part of the IPS. This should include:

- ✓ the legislation that grants them this power, and whether or not they utilise ADM to provide information and services to the public
- ✓ the types of ADM they use to make automated decisions, not just that AI is being used by the agency

- ✓ both a list of decisions they use ADM for, as well as relevant and easy to understand examples where possible, so the public can better understand how ADM is being used to make decisions that affect them
- ✓ any policies that clearly set out the principles for when and how they use ADM to make decisions and recommendations affecting members of the public.

As part of their IPS, agencies should clearly state the types of ADM they use to make automated decisions, not just artificial intelligence (AI) (i.e. from simple calculators to machine learning).

The list above may be used by agencies when considering the kinds of personal information and kinds of decisions that should be included in their privacy policies to comply with APP 1.7-1.9.

Where an agency is required to publish information about their use of ADM to make decisions that significantly affect the rights or interests or interests of individuals under the IPS that require the use of individuals' personal information, they may crosslink this disclosure to information on the kinds of personal information and kinds of decisions detailed in their APP privacy policy in accordance with the transparency obligation.

Example 1 – Interactions between the transparency obligation and FOI Act

The National Aged-Care Insurance Agency (NACIA) makes decisions about eligibility for elderly people trying to access health and aged-care support. NACIA is within scope of the ADM obligation because its staff use a generative AI chatbot, GPTea, to summarise candidate profiles and receive recommendations about eligibility to make assessments for support quicker.

NACIA provides a clear disclosure in its APP privacy policy that it uses a generative AI program which processes individuals' personal information including name, address, previous evaluations for government age care services, and health information for decision making and administrative actions to determine eligibility for age care support services and service delivery.

Separately, NACIA publishes information about how it makes eligibility decisions for aged care support as required by the Information Publication Scheme (IPS) in Part II of the FOI Act.

Specifically, the NACIA's 'IPS entry' or 'IPS page' on its website can comply with the IPS by explaining that the NACIA may use AI in making automated decisions to in relation to an individual's eligibility for age care support services under the relevant statute that governs NACIA's functions based on information provided by an applicant. This is cross-linked to NACIA's privacy policy.

How should agencies consider administrative law in the context of APP 1.7-1.9?

Administrative decisions, including those that are automated, must comply with existing legal requirements. Administrative decisions can be challenged through merits review, judicial review, Ombudsman complaints and engagement with the decision-maker.

Agencies should consider the scope of the ADM obligation in light of the meaning of 'decision' within section 4 of the *Administrative Review Tribunal Act 2024* (Cth) which includes the following:

- a) making, suspending, revoking or refusing to make an order or determination;

- b) giving, suspending, revoking or refusing to give a certificate, direction, approval, consent or permission;
- c) issuing, suspending, revoking or refusing to issue a licence, authority or other instrument;
- d) imposing a condition or restriction;
- e) making a declaration, demand or requirement;
- f) retaining, or refusing to deliver up, an article;
- g) doing or refusing to do any other act or thing.

In this regard, we note that most decisions performed by computer programs that fall within the abovementioned definition are likely to significantly affect the rights and interests of an individual.

How does the transparency obligation align with the Policy for the responsible use of AI in government?

The [Policy for the responsible use of AI in government](#) (the AI Policy) supports government agencies to safely and responsibly adopt AI. The AI policy applies to all non-corporate Commonwealth entities (NCEs), with some exceptions for the defence portfolio and national intelligence community. It can also be implemented voluntarily by agencies outside its scope.¹

To support public transparency, the AI policy requires in scope agencies to make a [publicly available statement](#) outlining their approach to AI adoption and use, as prescribed under the [Standard for AI transparency statements](#). An agency's AI transparency statement must provide information on instances where the public may directly interact with or be significantly impacted by the agency's use of AI, and classify their AI use according to usage patterns and domains.²

Decisions made by computer programs that do not involve the use of AI, as defined in the AI policy, do not need to be reflected in an agency's AI transparency statement.³

Aligned reporting requirements

Where AI systems are used to make decisions, agencies subject to the AI policy need to be transparent about this in both their AI transparency statement and their APP privacy policy. Agencies are encouraged to provide links between their privacy policy and their AI transparency statement.

Agencies may consider the information they provide in their AI transparency statement to provide information on the kinds of personal information and decisions made by computer programs that may significantly affect the rights and interests of an individual in their APP privacy policy and meeting their obligations under APP 1.7-1.9. However, the level of detail provided must be meaningful to a reasonable person.

¹ Digital Transformation Agency, *Policy for the responsible use of AI in government - Version 2.0*, <<https://www.digital.gov.au/ai/ai-in-government-policy>>.

² Digital Transformation Agency, *Standard for AI transparency statements*, <<https://www.digital.gov.au/ai/ai-in-government-policy/standard-ai-transparency-statements>>.

³ Digital Transformation Agency, *Policy for the responsible use of AI in government - Version 2.0: Appendices*, <<https://www.digital.gov.au/ai/ai-in-government-policy/appendices>>.

For example, an agency using AI to make eligibility decisions for government support payments may classify this under the usage pattern ‘Decision-making and administrative action’ and provide a brief overview in their AI transparency statement.

However, this level of detail would not be sufficient for an agencies’ privacy policy to comply with APP 1.7-1.9 as the agency may use multiple computer programs (including AI) to make eligibility decisions for government support payments for the purpose of ‘decision-making and administrative action’. The OAIC would expect an agency’s privacy policy to expand upon the detail included in their AI transparency statement to note that it relates to the provision of government support payments.

Example 2 – Application of transparency obligation to agencies using multiple computer programs (including AI)

The Immigration and Border Protection Authority (IBPA) integrates a range of computer programs to support the delivery of a range of statutory decisions within its remit. This includes decisions relating to the approval or refusal of visas, issuance or rejection of customs and trade clearances, and enforcement of travel restrictions and determinations.

The IBPA has integrated a range of computer program outputs into a centralised platform to enable individuals and goods to be processed through border entry points more efficiently.

In particular, the IBPA operates facial recognition technology at airports for border control purposes, as well as other image processing tools which rely on AI capabilities to enable image extraction from passports and detect objects which may require inspection by customs staff. These technologies integrate with separate computer programs such as those used to support the issuance of visa approvals and rejections, and risk scoring systems which flag potential security abnormalities for further investigation by human decision makers. These computer programs significantly impact the rights or interests of individuals as they determine whether an individual can pass through an Australian border checkpoint when entering or departing the country.

In complying with APP 1.7-1.9 obligations, IBPA demonstrates compliance with the transparency obligation by providing the following information in a new section of its privacy policy.

Automated Decision Making

IBPA operates computer programs which require the use of the following kinds of personal information at border entry points to facilitate immigration and border protection decision-making and administrative action:

- *Identity information (name, address, phone number, date of birth, gender, nationality)*
- *Travel details*
- *Criminal record.*

This information is used by IBPA to make the following kinds of decisions under Australian law:

- *Issues visa approvals and rejections*
- *Permit entry and exit of individuals at Australian border entry points.*

IBPA operates computer programs which require the use of the following kinds of personal information at border entry points to facilitate image processing for immigration and border protection purposes:

- *Photographs*
- *Biometric templates (facial recognition biometrics).*

This information is used by IBPA to make the following kinds of decisions under Australian law:

- *Permit entry and exit of individuals at Australian border entry points*
- *Identify individuals on security watchlists and active alert lists.*

What is the relationship between the transparency obligation and other Automated Decision-Making reforms?

The Attorney-General's Department (AGD) is leading the development of a whole-of-government framework for the use of ADM. The OAIC will consider its guidance on the transparency requirements under APP 1.7-1.9 as this work develops.