

Chapter 1:

Australian Privacy Principle 1 — Open and transparent management of personal information

Version 2.0, September 2026

Contents

Key points	3
What does APP 1 say?	3
Implementing practices, procedures and systems to ensure APP compliance	4
Developing an APP Privacy Policy	5
Information that must be included in an APP Privacy Policy	6
Kinds of personal information collected and held	7
How personal information is collected and held	7
Purposes for which the entity collects, holds, uses and discloses personal information	7
Accessing and seeking correction of personal information	7
Complaints about a breach of the APPs or a binding registered APP code	8
Likely overseas disclosures.....	9
Information relating to decisions made by a computer program.....	9
Other matters for inclusion in an APP Privacy Policy	18
Making an APP Privacy Policy publicly available	19
Making an APP Privacy Policy available free of charge and in an appropriate form	19
Making an APP Privacy Policy available in a requested form	20

Key points

- APP 1 outlines the requirements for an APP entity to manage personal information in an open and transparent way.
- An APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.
- An APP entity must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.
- An APP entity must take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website).
- An APP entity must, upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.
- An APP entity must include additional information in its APP Privacy Policy if it arranges for a computer program to use personal information to make, or do a thing that is substantially and directly related to making, a decision, that could reasonably be expected to significantly affect the rights or interests of an individual.

What does APP 1 say?

- 1.1 The declared object of APP 1 is ‘to ensure that APP entities manage personal information in an open and transparent way’ (APP 1.1). This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.
- 1.2 APP 1 imposes obligations upon an APP entity to:
 - take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2)
 - have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4)
 - take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6)
 - require entities to include additional information relating to automated decisions in an entity’s privacy policy (APP 1.7-1.9).
- 1.3 APP 1 lays down the first step in the information lifecycle – planning and explaining how personal information will be handled before it is collected. APP entities will be better placed to meet their privacy obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices.

Implementing practices, procedures and systems to ensure APP compliance

- 1.4 APP 1.2 requires an APP entity to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that will:
 - ensure the entity complies with the APPs and any binding registered APP code (see Part IIIB), and
 - enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs and any binding registered APP code.
- 1.5 APP 1.2 imposes a distinct and separate obligation upon an APP entity, in addition to being a general statement of its obligation to comply with other APPs. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation is a constant one. An entity could consider keeping a record of the steps taken to comply with APP 1.2, to demonstrate that personal information is managed in an open and transparent way.
- 1.6 The requirement to implement practices, procedures and systems is qualified by a 'reasonable steps' test. The reasonable steps that an APP entity should take will depend upon circumstances that include:
 - the nature of the personal information held. More rigorous steps may be required as the amount and sensitivity of personal information handled by an APP entity increases
 - the possible adverse consequences for an individual if their personal information is not handled as required by the APPs. More rigorous steps may be required as the risk and severity of possible adverse consequences increases
 - the nature of the APP entity. Relevant considerations include an entity's size, resources and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised entity, and
 - the practicability, including time and cost of implementing practices, procedures and systems. The 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to an APP entity. However, an entity is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.
- 1.7 The following are given as examples of practices, procedures and systems that an APP entity should consider implementing:
 - procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification
 - security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails) (see also Chapter 11 (APP 11))
 - a commitment to conducting a Privacy Impact Assessment (PIA) for new projects in which personal information will be handled, or when a change is proposed to information handling

practices. Whether a PIA is appropriate will depend on a project's size, complexity and scope, and the extent to which personal information will be collected, used or disclosed¹

- procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries²
- procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the entity in particular circumstances (see also Chapter 2 (APP 2))
- governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and regular reporting to the entity's governance body)
- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2
- appropriate supervision of staff regularly handling personal information, and reinforcement of the entity's APP 1.2 practices, procedures and systems
- mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs, and
- a program of proactive review and audit of the adequacy and currency of the entity's APP Privacy Policy and of the practices, procedures and systems implemented under APP 1.2.

Developing an APP Privacy Policy

- 1.8 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. At a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity. As the policy will usually be available on the entity's website (see paragraph 1.37), it should be written in a style and length that makes it suitable for web publication.³
- 1.9 An APP entity should regularly review and update its APP Privacy Policy to ensure that it reflects the entity's information handling practices. This review could, at a minimum, be undertaken as part of an entity's annual planning processes. An entity could also:
 - include a notation on the policy indicating when it was last updated
 - invite comment on the policy to evaluate its effectiveness, and explain how any comments will be dealt with
- 1.10 An APP Privacy Policy should explain how the APP entity manages the personal information it collects, and the information flows associated with that personal information. This reflects the central object of APP 1, which is to ensure that entities manage personal information in an open and transparent manner. The policy is not expected to contain detail about all the

¹ Further information about Privacy Impact Assessments is contained in OAIC, Guide to Undertaking Privacy Impact Assessments, OAIC website <<https://www.oaic.gov.au>>.

² For example, see OAIC, Data Breach Preparation and Response, OAIC website <<https://www.oaic.gov.au>>.

³ The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services, see OAIC, Mobile Privacy: A Better Practice Guide for Mobile App Developers, OAIC website <<https://www.oaic.gov.au>>.

practices, procedures and systems adopted to ensure APP compliance. The policy also differs from a collection notice provided to an individual under APP 5.1, which will provide specific information relevant to a particular collection of personal information (see Chapter 5 (APP 5)).

- 1.11 It is open to an APP entity to choose the style and format for its APP Privacy Policy, so long as the policy is clearly expressed, up-to-date and otherwise complies with the requirements of APP 1.
- 1.12 Where an APP Privacy Policy is made available online, using a layered approach to the provision of the information may assist an individual's understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy.⁴
- 1.13 An APP Privacy Policy should be tailored to the specific information handling practices of an entity. For example, for a large APP entity where distinct business units handle personal information differently, it may be appropriate for the entity to have a set of policies to cover the different types of personal information handled or different information handling practices.
- 1.14 The APP Privacy Policy should be directed to the different audiences who may consult it. Primarily this will be individuals whose personal information is, or is likely to be, collected or held by the APP entity. If personal information relevant to particular classes of people or segments of the community is handled differently within the entity, this could be explained and signposted by headings. For example, different practices may be adopted in the entity for handling personal information relating to young people or people with a disability.

Information that must be included in an APP Privacy Policy

- 1.15 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy:
 - the kinds of personal information collected and held by the entity (APP 1.4(a))
 - how personal information is collected and held (APP 1.4(b))
 - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c))
 - how an individual may access their personal information and seek its correction (APP 1.4(d))
 - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)), and
 - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy (APP 1.4(g)).
- 1.16 Entities must also include information if it arranges for a computer program to use personal information to make, or do a thing that is substantially and directly related to making, a decision, that could reasonably be expected to significantly affect the rights or interests of an individual (APP 1.7-1.9).
- 1.17 Further guidance is set out below.

⁴ For an example of a layered approach, see OAIC, Privacy Policy Summary, OAIC website <<https://www.oaic.gov.au>>.

Kinds of personal information collected and held

- 1.18 An APP Privacy Policy must describe in general terms the kinds of personal information an APP entity usually collects and holds (APP 1.4(a)). The terms ‘collects’ and ‘holds’ are discussed in Chapter B (Key concepts). For example, the policy may list personal information holdings as ‘contact details’, ‘employment history’, ‘educational qualifications’ and ‘complaint details’.
- 1.19 ‘Sensitive information’ collected or held by the entity could be separately listed (‘sensitive information’ is defined in s 6(1) and discussed in Chapter B (Key concepts)). For example, a policy may list sensitive information relating to ‘health information about an individual’, ‘racial or ethnic origin’, ‘criminal records’, ‘religious affiliation’ and ‘political opinions.’

How personal information is collected and held

- 1.20 An APP Privacy Policy must explain an APP entity’s usual approach to collecting personal information (APP 1.4(b)). For example, the policy may explain whether personal information is collected directly from individuals or from list purchases, competitions, or referrals from individuals or other entities.
- 1.21 The policy must describe an APP entity’s usual approach to holding personal information. This should include how the entity stores and secures personal information. For example, the policy may explain that personal information is stored by a third party data storage provider, or is combined or linked to other information held about an individual. The description of security measures should not provide details that jeopardise the effectiveness of those measures.

Purposes for which the entity collects, holds, uses and discloses personal information

- 1.22 An APP Privacy Policy must describe the purposes for which personal information is usually collected, held, used and disclosed (APP 1.4(c)). An APP entity is not expected to publish details of purposes that form part of normal internal business practices, such as auditing, business planning, billing, and de-identifying personal information. The description of purposes could indicate the range of people or entities to which personal information is usually disclosed, and details about an entity’s functions or activities that involve personal information that are contracted out. An organisation could also indicate if personal information is shared with a related body corporate.⁵ Discussion of the terms ‘purpose’, ‘collects’, ‘holds’, ‘uses’ and ‘discloses’ is in Chapter B (Key concepts).

Accessing and seeking correction of personal information

- 1.23 An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state:
- that individuals have a right to request access to their personal information and to request its correction (APPs 12 and 13), and

⁵ Section 13B of the Privacy Act permits ‘related bodies corporate’ to share personal information in some circumstances. Related bodies corporate are discussed in Chapter B (Key concepts). The sharing of information between related bodies corporate is discussed in Chapter 3 (APP 3) and Chapter 6 (APP 6).

- the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).⁶
- 1.24 If an APP entity wishes an individual to follow a particular procedure in requesting access to or correction of their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity's APP Privacy Policy. However, an APP entity cannot require the individual to follow a particular procedure to make the access or correction request (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).
 - 1.25 An agency's APP Privacy Policy could also refer to the *Freedom of Information Act 1982* (FOI Act) and explain that the access and correction requirements in the Privacy Act operate alongside and do not replace other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information, including the FOI Act (this is discussed in more detail in Chapter 12 (APP 12) and Chapter 13 (APP 13)).
 - 1.26 An APP entity may have other specific access or correction obligations outside the Privacy Act (for example the Consumer Data Right under Part IVD of the *Competition and Consumer Act 2010*). In such cases, the APP entity could also refer or explain those obligations where appropriate.

Complaints about a breach of the APPs or a binding registered APP code

- 1.27 An APP Privacy Policy must explain how an individual can complain about an APP entity's breach of the APPs or a binding registered APP code (APP 1.4(e)). It is implicit in this requirement that an entity which is bound by a binding, registered APP code should clearly state that fact and name the code.
- 1.28 Details that should also be included in the APP Privacy Policy are the procedure and contact details for complaining directly to the APP entity (see for example, the generic contact details in paragraph 1.22) and, where applicable, the procedure for complaining to an external complaint body (such as an external dispute resolution scheme of which the entity is a member and that is recognised by the Information Commissioner).⁷ The policy could inform individuals of the different stages in complaint handling: in most cases, a complaint should first be made in writing to the entity, as required by s 40(1A), and that the entity should be given a reasonable time (usually 30 days) to respond; following engagement with the entity, a complaint may be taken to a recognised external dispute resolution scheme of which the entity is a member; and, after those avenues have been considered, a complaint may be taken to the OAIC.
- 1.29 The policy could refer to other complaint avenues that operate alongside the Privacy Act. For example, banks are required to provide information to customers about complaint handling and dispute resolution in relation to the bank's obligations under the *Corporations Act 2001*,

⁶ The OAIC has published guidance for agencies about developing their access to information webpages. This includes recommendations about adopting an 'Access to information' icon. This guidance may assist agencies in developing online access and correction processes, which could then be explained in the APP Privacy Policy under APP 1.4(d). See OAIC, Guidance for Agency Websites: 'Access to Information' Web Page, OAIC website <<https://www.oaic.gov.au>>.

⁷ Further information about external dispute resolution schemes recognised by the Information Commissioner is available in OAIC, Guidelines for Recognising External Dispute Resolution Schemes, OAIC website <<https://www.oaic.gov.au>>.

the Code of Banking Practice, and the Electronic Funds Transfer Code of Conduct. In these circumstances, the APP Privacy Policy could note the different procedures for privacy and non-privacy complaints (or link to other explanatory material the APP entity has published).

Likely overseas disclosures

- 1.30 An APP Privacy Policy must set out whether personal information is likely to be disclosed to overseas recipients and the countries in which such recipients are likely to be located ‘if it is practicable to specify those countries in the policy’ (APP 1.4(f) and 1.4(g)). This includes a likely disclosure to a related body corporate located overseas, and the country in which that body is located. An APP entity can be regarded as likely to disclose personal information to an overseas recipient if it is the entity’s current practice or it has established plans to do so.
- 1.31 An APP entity is required to set out in the policy only likely disclosures of personal information to overseas recipients, and not likely uses of personal information by the entity. For example, routing personal information, in transit, through a server located outside Australia would usually be considered a ‘use’.⁸ Similarly, it would also be a use and not a disclosure for an entity to make personal information accessible to an overseas office of the entity, such as a consular office.⁹ For further discussion of the requirements applying to a cross-border disclosure of personal information, and what is considered a disclosure, see Chapter 8 (APP 8).
- 1.32 An example of when it may be impracticable to specify the countries in which overseas recipients of personal information are likely to be located is where personal information is likely to be disclosed to numerous overseas recipients and the burden of determining where those recipients are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an APP entity is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. As in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.
- 1.33 If personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the APP Privacy Policy rather than in the body of the policy. Another option in these circumstances may be to include a link in the APP Privacy Policy to a regularly updated list of those countries, accessible from the APP entity’s website. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).
- 1.34 This requirement to describe overseas disclosure practices in an APP Privacy Policy complements the obligation on an APP entity under APP 5.2(j) and (i) to notify an individual when personal information is being collected if the personal information is likely to be disclosed to overseas recipients and the location of those recipients (see Chapter 5 (APP 5)).

Information relating to decisions made by a computer program

- 1.35 From 10 December 2026, APP 1.7 requires APP entities to include the information outlined in APP 1.8 in their APP Privacy Policy if:

⁸ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

⁹ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

- the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making a decision (APP 1.7(a)); and
 - the decision could reasonably be expected to significantly affect the rights or interests of an individual (APP 1.7(b)); and
 - personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision (APP 1.7(c)).
- 1.36 APP 1.8 outlines the information which must be included in an entity's APP Privacy Policy if the conditions in APP 1.7 are met. This includes:
- the kinds of personal information used in the operation of such computer programs; and
 - the kinds of such decisions made solely by the operation of such computer programs; and
 - the kinds of such decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.

What is a decision?

- 1.37 For the purposes of APP 1.7 and 1.8, APP 1.9 states that:
- making a decision includes refusing or failing to make a decision; and
 - doing a thing includes refusing or failing to do a thing; and
 - a decision may affect the rights or interests of an individual, whether the rights or interests of the individual are adversely or beneficially affected.
- 1.38 The decisions must be a decision that 'could reasonably be expected to significantly affect the rights or interests of an individual (APP 1.7(b)).
- 1.39 As APP 1.9 sets out, the meaning of 'decision' is broad and can be something an entity chooses to do or chooses not to do. These include:
- making a decision – choosing to take an action or not take an action
 - doing something – including deliberately doing something or failing/refusing to do something
 - a decision that affects a person – where the outcome could reasonably be expected to benefit or disadvantage that individual.
- 1.40 For the avoidance of doubt, where a human decision-maker has made the decision, or done a thing related to making the decision, and has used a computer program for purposes other than facilitating the decision-making (such as using a word processing program to document a decision), this will not be captured.¹⁰

Example A: Glowride, a rideshare company, uses a computer program to analyse customer's personal information to manage the customer's ongoing usage of the service, including feedback or payment data or ratings provided by ride share drivers. One of the actions the computer program can execute is to suspend a user's account.

¹⁰ Paragraph 339 of the *Privacy and Other Legislation Amendment Act 2024* (Cth) Explanatory Memorandum

While a decision to suspend a customer's account may have a relatively minor impact on some customers, for a customer experiencing vulnerability who relies on Glowride to attend medical appointments, access essential services or maintain employment, the decision could significantly affect their rights or interests.

The example demonstrates that for a decision to be one that could reasonably be expected to significantly affect the rights or interests of an individual, it will depend on the individual's circumstances (such as a child or a person experiencing vulnerability). The effects of a decision must be more than trivial and must have the potential to significantly influence the circumstances of the individual concerned.

1.41 Other examples of the kinds of decisions that may affect the rights or interests of an individual include:¹¹

- a decision made under a provision of an Act or a legislative instrument to grant, or to refuse to grant, a benefit to the individual. For example, this may include a decision in relation to granting admission to a country or entitlement to a housing benefit.
- a decision that affects the individual's rights under a contract, agreement or arrangement. For example, this may include a contract for a life insurance policy.
- a decision that affects the individual's access to a significant service or support. For example, this may include access to healthcare services.

Importantly, a decision may be within scope of the APP 1.7-1.9 transparency obligation even where a computer program output does not replace the entire decision-making process or is subject to human review.

'Arranged for'

1.42 APP 1.7(a) uses the wording, 'the entity has arranged for a computer program'.

1.43 The words 'arranged for' clarify that it is the entity responsible for arranging the computer program to make, or do a thing that is substantially and directly related to making, a decision, which must meet the requirements in APP 1.7. (**Example B and C**)

1.44 This recognises that a computer program may be operated by one entity, but another entity is responsible for arranging for the computer program to make, or do a thing that is substantially and directly related to making, a decision. (**Example D**)

Example B: An employer permits or directs employees to use an artificial intelligence (AI) chat tool to draft performance assessments that determine promotion decisions.

Example C: An entity contracts a third-party software company to automatically approve or decline refunds on its behalf.

Example D: The National Taxation Authority (NTA) uses a third-party software called EzyTax to consider individual applications for their eligibility for a tax refund. EzyTax automatically approves or rejects the applications on behalf of the NTA depending on the personal

¹¹ APP 1.9(d) and paragraph 343 of the Explanatory Memorandum

information provided by the individual. The NTA has *arranged for* the EzyTax software to make decisions on its behalf.

The OAIC generally expects that the APP 1.7-1.9 transparency obligation typically remains with the APP entity who is using personal information to make a decision or do a thing that significantly affects the rights or interests of an individual.

- 1.45 APP entities should actively identify, assess and keep oversight over the third-party computer programs that they use to make a decision, both during and after procurement. Amongst other considerations, entities should understand how a computer program is being used in a third-party product or service to make or assist decisions and what types of decisions are being made. In this regard, APP entities and third-party computer program providers should ensure their contractual arrangements are clear regarding which entity maintains ultimate decision-making capability or judgement.

Privacy Tip: APP entities should be aware of the impact of any contractual arrangements they have with other entities when considering their APP 1.7 obligations. APP entities may still be required to comply with APP 1.7 where they have a contractual arrangement in place with another entity who provides them with a computer program.

The OAIC outlines below a non-exhaustive list of examples that would generally be considered ‘arranged for’ for the purposes of the APP 1.7-1.9 transparency obligation:

- an entity procures another entity’s AI system to screen and rank job applications leading to a decision being made on who to employ
- an employer permits or directs employees to use an AI chat tool to draft performance assessments that determine promotion decisions
- an entity contracts a third-party software company to automatically approve or decline refunds on its behalf
- an entity has a case management system that automatically escalates particular types of complaints.

‘Computer program’

- 1.46 The meaning of computer program is intended to be interpreted broadly.
- 1.47 The term ‘computer program’ is intended to take its ordinary meaning and encompass a broad range of matters, including pre-programmed rule-based processes, artificial intelligence and machine learning processes to make a computer execute a task.¹²

A wide range of technologies are likely to fall within the definition of computer program, including commonly-used software, apps, or word-processing tools. Generative AI tools used to generate text, images, videos, code or synthesis, including chatbots and other types of AI

¹² Paragraph 336 of the Explanatory Memorandum

all fall within the definition of computer program for the purpose of the APP 1.7-1.9 transparency obligation.

'Substantially and directly related to making a decision'

- 1.48 Under APP 1.7, an APP Privacy Policy must contain the information outlined in APP 1.8 if, amongst other things, the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making a decision (APP 1.7(a)).
- 1.49 The use of the words 'do a thing that is substantially and directly related to making a decision' in APP 1.7(a) reflects that a computer program may be used to recommend a decision to a human decision-maker or guide a human decision-maker.¹³
- 1.50 Where a computer program is used to recommend a decision to a human decision-maker, or guide a human decision-maker, the thing must be substantially and directly related to making a decision to be captured:
- *substantially* means where it is a key factor in facilitating the human's decision making
 - *directly* means where the thing has a direct connection with making the decision.¹⁴
- 1.51 In addition, the OAIC considers that substantial means 'real or of substance and not insubstantial or nominal'.¹⁵
- 1.52 A computer program may be substantially and directly related to making a decision regardless of whether the nature of the output is advisory or determinative. When considering if an advisory output is within scope of this limb of the APP 1.7-1.9 transparency obligation, APP entities should consider factors including:
- which part of the decision-making process the computer program was used for
 - the sources of information used to generate the output
 - the parameters provided to the computer program to generate a decision
 - how the computer program output ultimately influenced the human decision-maker's judgement.

Example of factors to determine whether a computer program is doing a thing that is substantially and directly related to making a decision

- 1.53 An APP entity may consider this non-exhaustive list of factors to enable it to assess whether a computer program substantially facilitates and is directly connected to a human decision-maker's decision:
- degree of reliance on the computer program output (**Example E**)

¹³ Paragraph 337 of the Explanatory Memorandum

¹⁴ Ibid.

¹⁵ See *Tillmanns Butcheries Pty Ltd v Australasian Meat Employees Union & Ors* [1979] FCA 85 - external site[14]–[15]; (1979) 27 ALR 367 [383]; per Deane J in relation to the meaning of 'substantial loss' in s 45D of the Trade Practices Act 1974. Although Deane J noted that it was unnecessary that he form a concluded view, Deane J's interpretation of 'substantial' provides general guidance on the interpretation of this term under the FOI Act. See also for example *Re Marko Ascic v Australian Federal Police* [1986] FCA 260.

- for example, the higher the reliance, the higher the likelihood of the computer program output being determinative rather than advisory
- ability and likelihood of human override over a computer program output (**Example F**)
- nature of the output (advisory vs determinative) (**Example G**)
- transparency and explainability of outputs available to the decision-maker (what the computer program did and why) (**Example H**)
- integration and complexity of the computer program into the decision-making workflow (**Example I**).

Example E: A bank uses a computer program to assess loan applications. The loan officer relies heavily on the computer program's risk score and almost always follows its recommendation.

Example F: An online marketplace uses a computer program to suspend seller accounts if commission payments are not made by a seller within 60 days. Staff can overturn the algorithm's decision, however, because the computer program is considered highly accurate, staff rarely overturn the algorithm's decision.

Example G: A private tertiary education institute uses a computer program to rank scholarship applications. The computer program produces a recommendation, however, the scholarship panel makes the final decision and can disregard the ranking. The recommendation produced by the computer program is substantially and directly related to making a decision as the scholarship panel considers the ranking provided by the computer program even though they may choose to ignore it.

Example H: An insurance company uses a computer program to determine whether a claim should be rejected. The system provides the claims officer with a rejection decision but does not explain which information led to the outcome.

Example I: A rental company uses a computer program that automatically collects an applicant's information, calculates a suitability score and places the result directly into the employee's application assessment screen. The system is deeply integrated into the decision-making process.

- 1.54 The examples provided above demonstrate that a computer program does not necessarily need to make the final decision or to be the only decision-maker for a type of decision. An output can still substantially facilitate and be directly connected to a human decision where the human decision maker relies on or is significantly influenced by the computer program's output.

'Significantly affect the rights or interests of an individual'

- 1.55 Under APP 1.7, APP privacy policies must contain the information outlined in APP 1.8 if, amongst other things, the decision could reasonably be expected to significantly affect the rights or interests of an individual (APP 1.7(b)).
- 1.56 APP 1.9(c) outlines that a decision may affect the rights or interests of an individual, whether the rights or interests of the individual are adversely or beneficially affected.

- 1.57 *Significantly* means the impact of the decision or thing must be more than trivial and must have the potential to considerably influence the circumstances or outcomes for the individual concerned.
- 1.58 The circumstances of an individual may influence whether or not a decision could reasonably be expected to significantly affect the rights or interests of the individual, such as in the case of a child or vulnerable person.

Rights and Interests

- 1.59 In determining whether a decision could reasonably be expected to significantly affect the rights or interests of an individual, APP entities should consider adverse effects on rights and interests.
- 1.60 A *right* is a moral or legal entitlement to have or be able to do something.¹⁶ Australian law grants many legal rights which reflect human rights found in customary law, the Australian Constitution, statute law, common law, and international treaties to which Australia is a party. Rights afforded to Australians under these sources of law include:
- social and economic rights (e.g. housing, food, sanitation, healthcare, education, etc.)
 - civil and political rights (e.g. freedom of movement and assembly, freedom of expression, etc.)
- 1.61 An *interest* refers to a concern, benefit, stake or claim relating to something. In the context of the APP 1.7-1.9 transparency obligation, APP entities may consider a range of interests including legal, personal liberty, status, preservation of livelihood, personal and commercial reputation, property, employment, health, immigration, financial, commercial, behaviour choices and a child's interest in the provision of a supportive, safe and secure home.¹⁷
- 1.62 Other factors APP entities may consider when determining the likelihood that a decision could affect an individual's rights or interest may include the sensitive nature of the information used, whether they are dealing with vulnerable persons, whether there are any intrusive practices being used by the APP entity and if there are any significant financial outcomes involved.
- 1.63 The following examples of a decision 'could reasonably be expected to significantly affect the rights or interests of an individual':¹⁸
- a decision made under a provision of an Act or a legislative instrument to grant, or to refuse to grant, a benefit to the individual. For example, this may include a decision in relation to granting admission to a country or entitlement to a housing benefit
 - a decision that affects the individual's rights under a contract, agreement or arrangement. For example, this may include a contract for a life insurance policy

¹⁶ 'What are rights?', *Rights in Australia*, Parliamentary Education Office < <https://peo.gov.au/understand-our-parliament/how-parliament-works/system-of-government/rights-in-australia>>.

¹⁷ *Kioa v West* (1985) 159 CLR 550, Mason J at 582; Robin Creyke, John McMillan and Mark Smyth, *Control of Government Action: Text, Cases and Commentary* (Lexis Nexis Butterworths, 3rd ed, 2012) [10.1.9]; *L & Anor V State of South Australia*; *H-P V State of South Australia* [2017] SASCFC 133.

¹⁸ Paragraph 343 of the Explanatory Memorandum

- a decision that affects the individual's access to a significant service or support. For example, this may include access to healthcare services
- the use of computer programs to target individuals with content and advertisements may have a significant effect on an individual if, for example, it results in differential and/or personalised pricing for provision of, or access to, significant goods or services, or limits access to employment opportunities.

Example F: Life Insured is a life insurance company that has recently started to use an automated decision-making (ADM) software that has decreased employees' time for considering individual applications. The software being used allows employees to enter applicants' personal information and receive a decision of whether to approve or decline their life insurance policy in as little as 10 seconds. Although this software has improved the efficiency of Life Insured, they now must update their APP Privacy Policy to comply with APP 1.7 due to the software being used having a significant effect on the rights and interests of an individual.

Vulnerability

- 1.64 The circumstances of an individual may also influence whether or not a decision could reasonably be expected to significantly affect the rights or interests of the individual, such as in the case of a child or vulnerable person. The effects must be more than trivial and must have the potential to significantly influence the circumstances of the individual concerned.
- 1.65 Whether a person is a child or experiencing vulnerability is relevant, to the extent that a decision may have a greater impact on that person, as opposed to a person who is not a child or is not experiencing vulnerability. For example, a decision's effect on a child, individual from a low socio-economic background, Indigenous Australian, or person with a disability may be considered significant compared to its effect on other individuals.
- 1.66 When assessing vulnerability, APP entities should consider whether the decision in question produces an output that is materially different for a vulnerable cohort of individuals when compared to the general Australian population. Where this is the case, the computer program's decision should be taken to significantly affect the rights or interests of an individual.

The OAIC outlines below a non-exhaustive list of significant rights or interests that would generally be considered in scope of the obligation:

- access to essential food and nutrition
- access to healthcare, emergency or aged care services (including 'in home' services)
- access to physical assistance or support
- financial assistance
- access to educational services
- access to essential banking and credit services
- access to telecommunications
- access to essential utilities

- access to employment opportunities
- access to housing.

How much information should entities include in their privacy policy?

- 1.67 To ensure compliance with APP 1.7, 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.

Privacy Tip: Commercial-in-confidence information about automated decision-making systems is excluded from the requirement of APP 1.7.¹⁹ In this regard, the APP 1.7-1.9 transparency obligation does not require APP entities to include information in APP 1 privacy policies that is commercially sensitive information or would expose trade secrets.

The OAIC notes that in considering whether information is commercial-in-confidence, APP entities should classify information as falling in this category *only* if its release could harm an APP entity's commercial interests. The exclusion in APP 1.7 applies to the narrower category of 'commercial-in-confidence' information rather than information that has 'commercial value'.

For example, an APP entity may have a genuine financial interest in using a computer program to handle personal information to make decisions that significantly affect the rights or interests of an individual but would not be able to apply the commercial-in-confidence exclusion because the use of the program itself does not expose sensitive operational information about the entity.

- 1.68 Entities must ensure that meaningful and accessible information is provided to individuals.
- 1.69 Entities should strike an appropriate balance to ensure information is:
- articulated clearly and in plain language and easy to understand
 - structured to enable consumers to request further information, where required
 - appropriately tailored – sufficiently specific to be meaningful, while avoiding overwhelming levels of detail
 - organised so similar information is grouped in a logical manner
 - framed in a way that allows the information and the decision to be challenged or contested.
- 1.70 In complying with the APP 1.7-1.9 transparency obligation, APP entities may group information about the categories of decisions and types of personal information in their privacy policy to comply with the transparency obligation. However, the level of detail provided about these processes must be meaningful to a reasonable person.
- 1.71 Where an APP entity chooses to group information about categories of decisions and types of personal information used to inform a decision, this should be considered with regard to the sensitivity of the information relied upon by the computer program. Privacy policies

¹⁹ Addendum to the Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 38

should be able to clearly articulate where more sensitive types of information (e.g. health information or biometric templates) are used in the making of a computer's decision.

- 1.72 In circumstances where all decisions made by an entity rely on the use of the same type of personal information, APP entities are not required to separate out each decision on a granular basis in their privacy policy but should still consider presenting the information in ways that assist an individual's understanding.
- 1.73 For example, an APP entity may use a range of different computer programs for fraud detection, scam identification, and cybersecurity which may prevent access to significant goods or services. In this case, an APP privacy policy may outline it uses a range of fraud prevention technologies which process a individual's personal information (e.g. identity information, geolocation data, biometric information, and IP addresses) to decide whether to permit, flag or deny access to an account with the APP entity.

Government agencies' disclosure obligations under the Information Publication Scheme (IPS)

- 1.74 All Government agencies that are subject to the FOI Act are required to comply with obligations of disclosure under the Information Publication Scheme (IPS).
- 1.75 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. ADM information, that assists an agency to perform or exercise its functions or powers in making decisions or recommendations that affect the public, should be proactively published under the IPS.
- 1.76 Government agencies may consider cross linking IPS disclosures regarding ADM information with their APP 1.7 disclosure obligation.
- 1.77 [Part 13 of the FOI Guidelines](#) issued under section 93A of the FOI Act that agencies and ministers must have regard to when exercising a function or power provide further information on the IPS and associated considerations with the use of ADM systems and artificial intelligence.

Further guidance

- 1.78 For further guidance on APP 1.7-1.9, please refer to the following resources:
 - [APP 1.7-1.9 transparency obligation fact sheet \(PDF, 179 KB\)](#)
 - [APP 1.7-1.9 transparency obligation flowchart \(PDF, 246 KB\)](#)

Other matters for inclusion in an APP Privacy Policy

- 1.79 The list of matters that must be included in an APP Privacy Policy, as discussed above, is not exhaustive. In all cases, the policy should contain sufficient information to describe how the APP entity manages personal information.
- 1.80 The following are examples of other information that could be included:
 - any exemptions under the Privacy Act that apply to personal information held by the entity or to any of its acts or practices
 - whether the APP entity retains a record of personal information about all individuals (or categories of persons) with whom it deals

- who, other than the individual, can access personal information, and the conditions for access
- the entity's process or schedule for updating its APP Privacy Policy, and how changes will be publicised
- if the entity interacts with and collects personal information about a vulnerable segment of the community (such as children), the criteria that will be applied and the procedure that will be followed in collecting and holding that personal information
- the situations in which a person can deal with the entity by not identifying themselves or by using a pseudonym (see APP 2, Chapter 2)
- information retention or destruction practices or obligations specific to the entity.

Making an APP Privacy Policy publicly available

Making an APP Privacy Policy available free of charge and in an appropriate form

- 1.81 APP 1.5 requires an APP entity to take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form. This furthers the objective of APP 1 of ensuring personal information is managed in an open and transparent way.
- 1.82 An APP entity is generally expected to make its policy available by publishing it on its website (see Note to APP 1.5). The information in the policy may be provided using a layered approach (see paragraph 1.12 above). The policy should be prominently displayed, accessible and easy to download. For example, a prominent link or privacy icon, displayed on each page of the entity's website, could provide a direct link to the APP Privacy Policy. If it is foreseeable that the policy may be accessed by individuals with special needs (such as individuals with a vision impairment, or individuals from a non-English speaking background), appropriate accessibility measures should be available. Agencies are also required to comply with any applicable government or statutory accessibility requirements.²⁰
- 1.83 Online publication may not be appropriate in some circumstances, for example, where the APP entity does not have an online presence or where individuals who regularly interact with the entity may not have internet access. In these circumstances, options an entity should consider include:
- displaying the policy on a stand at the entity's premises so it can be seen by members of the public
 - distributing a printout of the policy on request
 - including details about how to access the policy at the bottom of all correspondence to individuals
 - where the entity interacts with individuals by telephone, informing them during the telephone call of how the policy may be accessed in a particular form.

²⁰ See, for example, Digital Service Standard Criteria — 9. Make It Accessible, DTA website <<https://www.dta.gov.au>>.

Making an APP Privacy Policy available in a requested form

- 1.84 APP 1.6 requires an APP entity, upon request, to take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the form requested. This should be done as soon as reasonably practicable after the request is received.
- 1.85 The reference to a ‘body’ requesting a copy of a policy makes it clear that a request may be made other than by an individual or entity that is subject to the Privacy Act.
- 1.86 An APP entity can decline to provide a copy of its APP Privacy Policy in a particular form if it would not be reasonable in the circumstances to meet the request. The steps that are reasonable will depend upon:
 - other steps taken by the entity to make its policy publicly available and accessible
 - the practicability, including time and cost involved. However, an entity is not excused from providing a copy in a particular form by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances
 - the sensitivity of the personal information held. More rigorous steps may be required where the entity holds ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature
 - whether the entity has unique or unusual information handling practices
 - any reasons given by the body or person for requesting the policy in a particular form, and
 - any accessibility or other specific needs of the body or person requesting the policy. For example, it may be reasonable to provide the policy in a form that can be accessed via assistive technology where appropriate.
- 1.87 Inherent in the obligation to take ‘reasonable steps’ is an expectation that an APP Privacy Policy will usually be made available free of charge. The cost of doing so should be treated as part of an APP entity’s normal operating costs. If a charge is imposed, the reason for the charge and the basis of calculation should be clearly communicated and explained before the policy is made available in the requested form, and the charge should be calculated at the lowest reasonable cost.
- 1.88 If a request for access in a particular form is declined, the APP entity should explain this decision to the person or body making the request. The entity should be prepared to undertake reasonable consultation with the requester about the request.