Australian Government

Office of the Australian Information Commissioner

Handling personal information when providing accredited Digital ID services

November 2026



OAIC

Contents

Handling personal information when providing accredited Digital ID services 2

Privacy obligations of an accredited entity 2

- Privacy safeguards in the Digital ID Act 3
- Privacy obligations in the Privacy Act 3

Collection 4

- Australian Privacy Principles 3, 4 and 5 4
- Prohibition on collecting certain attributes (section 44) 4

Use and Disclosure 5

- Australian Privacy Principles 6, 7, 8 and 9 5
- Express consent required for disclosure of certain attributes 5
- Disclosure of unique identifiers 7
- Prohibited marketing purposes 7
- Prohibition on data profiling to track online behaviour 8

Retention 9

- Prohibited retention of certain attributes 9

Destruction or de-identification 9

- Personal information obtained through the Australian Government Digital ID System (AGDIS) 9
- Personal information obtained through other digital ID systems 9

State and Territory privacy legislation 10

Table summarising the interaction between the Digital ID Act Privacy Safeguards and the Privacy Act Australian Privacy Principles 11

Handling personal information when providing accredited Digital ID services

This guidance piece focuses on an accredited entity's obligations for the collection, use, disclosure, retention and destruction of personal information when providing accredited Digital ID services.

Example: An individual engages with the Identity Service Provider (ISP), ID4U, for the purposes of setting up their Digital ID. The ISP, ID4U, will:



Collect
Personal information and identity documents from the individual
Personal information from issuing government agencies or other authoritative sources to verify and validate identity documents provided by the individual



Disclose
Personal information and details from identity documents to the authoritative source for the purposes of verifying that the document is real and owned by the individual



Use
An individual's personal information to generate and manage the individual's Digital ID.

Privacy obligations of an accredited entity

Privacy protections are built into Australia's Digital ID system. When providing accredited services, accredited entities must comply with the privacy safeguards in the *Digital ID Act 2024* (Digital ID Act). These safeguards are in addition to, and build on, the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Privacy Act) (or equivalent state or territory laws).

All accredited entities will be required to comply with the following privacy requirements:

Privacy obligations of an accredited entity
be subject to the federal Privacy Act or an comparable state or territory law or enter into an APP-equivalent agreement
comply with the federal Notifiable Data Breaches scheme, unless they are covered by a comparable state or territory scheme
comply with the 13 additional privacy safeguards in the Digital ID Act

Privacy safeguards in the Digital ID Act

The Digital ID Act contains 13 additional privacy safeguards that apply to all accredited entities and that build on the privacy safeguards contained in the Privacy Act (or equivalent state or territory laws). The 13 additional privacy safeguards:

- regulate accredited entities' handling of biometric information and certain attributes when providing accredited services;
- outline requirements to obtain express consent for the handling of biometric information and certain other attributes of individuals; and
- limit the handling of personal information for data profiling, enforcement purposes and marketing.

Privacy obligations in the Privacy Act

In addition to complying with the 13 additional privacy safeguards in the Digital ID Act, accredited entities will have to comply with privacy obligations in the Privacy Act, in particular the 13 APPs, when providing accredited services. This includes small business operators who are ordinarily exempt from complying with the Privacy Act for their broader personal information handling.

The Privacy Act obligations will not apply to accredited state or territory entities where the entity is subject to state or territory privacy legislation that provides protection comparable to the Privacy Act. Alternatively, accredited state or territory entities can enter into an APP-equivalent agreement with the Commonwealth.[1]

[1] s 34 and s 36(2)(c) of the Digital ID Act.

Collection

When collecting information (for example, information from an individual or from an authoritative source) an accredited entity must comply with section 44 of the *Digital ID Act 2024* (the Digital ID Act), rule 4.42(1) of the *Digital ID (Accreditation) Rules 2024*, as well as either the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) (the Privacy Act) or applicable State/Territory legislation.

Australian Privacy Principles 3, 4 and 5

APP 3 deals with two aspects of collecting solicited personal information: **when** an APP entity can collect personal information, and **how** an entity must collect personal information.

APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information (personal information received where the entity has taken no active steps to collect it).

APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.

See Chapter 3, Chapter 4 and Chapter 5 of the OAIC's APP Guidelines on its website for detailed guidance on these requirements.

Prohibition on collecting certain attributes (section 44)

Section 44 of the Digital ID Act (Collection of certain attributes prohibited) overrides the application of APP 3 for the collection of certain types of sensitive information.

While APP 3 generally allows the collection of the full range of sensitive information when certain criteria are met, section 44 overrides this by prohibiting the collection by an accredited entity of any of the following attributes of an individual:

Information or an opinion about an individual's:
✗ Racial or ethnic origin
✗ Political opinions
✗ Membership of a political association
✗ Religious beliefs or affiliations
✗ Philosophical beliefs
✗ Sexual orientation or practices

This prohibition does not apply if the accredited entity:

- did not solicit the attribute of the individual, and
- destroys the attribute, as soon as practicable, after becoming aware they have collected the attribute.

Use and Disclosure

An accredited entity must comply with APPs 6-9 in the Privacy Act (or applicable State/Territory legislation) when using and disclosing an individual's personal information as part of managing an individual's Digital ID, as well as sections 45, 46, 47, 53 and 55 of the Digital ID Act.

Australian Privacy Principles 6, 7, 8 and 9

APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.

APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.

APP 8 provides that before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[2]

APP 9 restricts the adoption, use and disclosure of government related identifiers by organisations.

See Chapter 6, Chapter 7, Chapter 8 and Chapter 9 of the OAIC's APP Guidelines on its website for detailed guidance on these requirements.

Express consent required for disclosure of certain attributes

When an accredited entity is verifying the identity of an individual or authenticating a Digital ID, the accredited entity must not disclose the below attributes of the individual to the relying party without the individual's express consent.[3] For this particular disclosure, the express consent requirement overrides APP 6 which would otherwise allow disclosure in a broader range of situations.

[2] Entities should also consider section 77 of the Digital ID Act, under which the Digital ID Rules may make provision in relation to the holding, storing, handling or transfer of information outside Australia if the information is or was generated, collected, held or stored by accredited entities within the AGDIS. As at 29 September 2026, no rules have been made under section 77, so APP 8 will continue to regulate the cross border disclosure of personal information in these circumstances.

[3] s 45 and s 46 of the Digital ID Act.

The following attributes must not be disclosed without an individual's express consent:
✕ Current name or former name
✕ Address
✕ Date of birth
✕ Phone number
✕ Email Address
✕ A restricted attribute (including health information about the individual, government issued identifiers, and information or an opinion about the individual's criminal record, membership of a professional or trade association or trade union).
✕ An attribute of a kind prescribed in the Accreditation Rules:[4] • attributes that are on a document or other credential listed in Schedules 1 to 4 of the Rules (to the extent not already captured above) • attributes that are derived from an attribute listed above (for example, whether an individual is aged over 18 is an attribute derived from the individual's date of birth) • a 'special attribute' of an individual[5] • an attribute that is self-asserted by the individual and not verified.

In addition, for restricted attributes, an accredited entity can only disclose a restricted attribute of an individual to a relying party that is not a participating relying party[6] if the entity's conditions on accreditation include an authorisation to disclose the restricted attribute to the relying party.

[4] See part 7.1 of the Digital ID (Accreditation) Rules.

[5] See rule 5.35 of the Digital ID (Accreditation) Rules.

[6] s 9 of the Digital ID Act: A relying party is a participating relying party if:

(a) the relying party holds an approval under section 62 to participate in the Australian Government Digital ID System; and
(b) the participation start day for the relying party has arrived or passed.

Disclosure of unique identifiers

An accredited entity that has assigned a unique identifier to an individual within Australia's Digital ID System must not disclose that unique identifier to another accredited entity or a relying party unless:

- the disclosure of the unique identifier is to a contractor engaged by the accredited entity, for the purposes of the contractor providing an accredited service of the accredited entity;[7]
- the unique identifier is disclosed to another entity if the other entity is facilitating access to the entity for whom the unique identifier was created;[8]
- detecting, reporting or investigating a contravention or alleged contravention of the Digital ID Act, standards or rules made under that Act or service levels determined under section 80;
- conducting proceedings in relation to a contravention or alleged contravention of a civil penalty provision of the Digital ID Act, standards or rules made under that Act or service levels determined under section 80;
- detecting, reporting or investigating either a Digital ID fraud incident or a cyber security incident within a digital ID system as defined in the Digital ID Act;
- conducting an assessment under paragraph 33C(1)(g) of the Privacy Act; and
- detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory.[9]

Prohibited marketing purposes

Personal information handled while providing accredited services in Australia's Digital ID System must not be used or disclosed for the following prohibited marketing purposes:[10]

Prohibited marketing purposes
offering to supply goods or services
advertising or promoting goods or services
enabling another entity to offer to supply goods or services

[7] s 47(5) of the Digital ID Act.

[8] s 47(5) of the Digital ID Act.

[9] Please see s 54 of the Digital ID Act for circumstances where use or disclosure of information for enforcement purposes is permitted. For further information also see Law enforcement access to Digital ID.

[10] s 55 of the Digital ID Act.

Prohibited marketing purposes
✗ enabling another entity to advertise or promote goods or services
✗ market research

The prohibition does not apply where the information about an individual is disclosed to the individual to whom the information relates (with their express consent) for the purposes of:

- offering to supply the entity's accredited services; or
- advertising or promoting the entity's accredited services.

This overrides the direct marketing prohibition in APP 7, where there are a broader range of exceptions where direct marketing can occur.

Prohibition on data profiling to track online behaviour

An accredited entity must not use or disclose personal information it holds about an individual, if the personal information is any of the following:[11]
✗ information about the services provided by the entity that the individual has accessed or attempted to access
✗ information relating to how or when access was obtained or attempted to be obtained by the individual
✗ information relating to the methods of access or attempted access by the individual
✗ the date and the time the individual's identity was verified.

The prohibition does not apply where the use or disclosure is:

- required or authorised by or under a law; or
- for the purposes of the accredited entity complying with the Digital ID Act; or
- for purposes relating to improving the performance or useability of the entity's information technology system used to provide its accredited services.

The individual's consent is not a relevant exception.

This obligation overrides the requirements in APP 6 because it only allows use or disclosure for this purpose in very limited circumstances.

For information about the use or disclosure of certain personal information for prohibited enforcement purposes, see Law enforcement access to Digital ID.

[11] s 53 of the Digital ID Act.

Retention

Prohibited retention of certain attributes

An accredited identity exchange provider must not retain the following attributes collected during an authenticated session:[12]

- name
- address
- date of birth
- phone number
- email Address
- a restricted attribute (includes health information about the individual, government-issued identifiers, and information or an opinion about the individual's criminal record, membership of a professional or trade association or trade union)
- an attribute of a kind prescribed in the Accreditation Rules.[13]

Destruction or de-identification

Personal information obtained through the Australian Government Digital ID System (AGDIS)

An accredited entity that holds or has held an approval to participate in AGDIS must destroy or de-identify personal information in its possession or control when:[14]

- the personal information was obtained by the entity through AGDIS;
- the entity is not required or authorised by law[15] to retain the information; and
- the personal information does not relate to any current or anticipated legal or dispute resolution proceedings to which the accredited entity is a party.

For information about destruction requirements for biometric information see Handling biometric information when providing accredited Digital ID services.

Personal information obtained through other digital ID systems

Where an accredited entity, subject to the Privacy Act, handles personal information that was obtained through a digital ID system other than AGDIS, the accredited entity must comply with their existing privacy obligations in relation to destruction or de-identification.

---

[12] Rule 1.6 Digital ID (Accreditation) Rules: An authenticated session means a persistent interaction between 2 entities involved in a transaction in a digital ID system which begins with an authentication event and ends with an event that brings the authenticated session to an end.

[13] s 56 of the Digital ID Act.

[14] s 136 of the Digital ID Act.

[15] This includes the Digital ID Act and related rules but excludes any prescribed laws.

Destruction or de-identification obligations are set out in APP 11.2 which provides that, where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed, the entity must take reasonable steps to destroy the information or ensure that it is de-identified.

For information about destruction requirements for biometric information see Handling biometric information when providing accredited Digital ID services.

See Chapter 11 of the OAIC's APP Guidelines on its website for detailed guidance on these requirements.

State and Territory privacy legislation

Accredited entities bound by comparable State or Territory privacy legislation rather than the APPs, should refer to their State or Territory regulator for further information about these obligations.

Table summarising the interaction between the Digital ID Act Privacy Safeguards and the Privacy Act Australian Privacy Principles

The following table provides a brief outline of how each Digital ID privacy safeguard and relevant APPs interact. For further information on the mandatory requirements of the APPs, see the OAIC's Australian Privacy Principles guidelines**.**

Safeguard	Relevant APP	Interaction between safeguard and APP
Section 44: Prohibition on collection of certain attributes	Collection – APPs 3 and 4	S 44 overrides[16] APP 3.3 and 3.4 in relation to the collection of attributes listed in s 44. For other types of sensitive information that are not listed in s 44, APP 3.3 and 3.4 will apply to collection.
Section 45: Express consent for disclosure of certain attributes to relying parties	Disclosure – APP 6	For disclosure of the specified attributes listed in s 45, the provision sets out how disclosure can occur and overrides the operation of APP 6 as express consent is the only basis for disclosure of these attributes to relying parties.
Section 46: Prohibition of disclosure of restricted attributes without express consent	Disclosure – APP 6	For disclosure of restricted attributes of individuals to relying parties, s 46 will override the operation of APP 6 as express consent is the only basis for disclosing these attributes.
Section 47: Restriction of disclosure of unique identifiers	Disclosure – APP 6	The restrictions in s 47 on disclosing a unique identifier override the operation of APP 6.
Sections 48 – 52: Sections governing the handling of	Collection – APP 3 Disclosure – APP 6	S 48 prohibits the handling of biometric information unless the handling is specifically authorised by ss 49 and 50, and in some cases, only if express consent is also obtained. Due to

[16] For the purposes of this guidance, 'overrides' is used to convey situations where a safeguard imposes stricter requirements than the corresponding APPs. This term does not alter the legal position that both the Digital ID Act and the Privacy Act apply concurrently.

Safeguard	Relevant APP	Interaction between safeguard and APP
biometric information	Retention and Destruction– APP 11.2	their prescriptive nature, these sections override APPs 3, 6 and 11.1 in relation to the handling of biometric information. S 51 overrides APP 11.2 in relation to the retention and destruction of biometric information as it contains specific timeframes for destruction which are more immediate than those set out in APP 11.2. It also requires destruction rather than allowing de-identification as an alternative.
Section 53: Prohibition on data profiling to track online behaviour	Disclosure – APP 6	S 53 overrides APP 6 by providing only a very limited number of exceptions at subsection 53(3) where online behavioural data can be used or disclosed by the accredited entity.
Section 54: Prohibition on handling of personal information for enforcement purposes	Disclosure – APP 6	By restricting the use and disclosure of personal information for enforcement related activities to a limited number of prescribed circumstances, s 54 overrides APP 6 which allows personal information to be handled in a broader range of situations.
Section 55: Prohibition on handling personal information for marketing purposes	Direct Marketing – APP 7	S 55 overrides APP 7 by only allowing handling of personal information for marketing purposes, where the information is disclosed to an individual for the purposes of offering to supply the entity's accredited services, or advertising or promoting those services, and the information is disclosed to the individual with their express consent.
Section 56: Prohibition on the retention of certain attributes by an accredited identity exchange provider	Destruction – APP 11.2	S 56 overrides APP 11.2 for accredited identity exchange providers in relation to the retention of certain attributes, by prohibiting retention after the end of an authentication session (as defined in the Digital ID (Accreditation) Rules 2024) rather than applying a 'reasonable steps' requirement as set out in APP 11.2.
Section 136: Destruction or de-	Destruction – APP 11.2	S 136 overrides APP 11.2 for accredited entities that hold an approval to participate in the

Safeguard	Relevant APP	Interaction between safeguard and APP
identification of information by AGDIS participants		AGDIS (or whose approval is suspended/revoked) in relation to the information outlined in the section.