



Handling personal information when providing accredited Digital ID services

Contents

Handling personal information when providing accredited Digital ID services	1
Collection	1
Australian Privacy Principles 3, 4 and 5	1
Prohibition on collecting certain attributes (section 44)	2
Use and Disclosure	3
Australian Privacy Principles 6, 7, 8 and 9	3
Express consent required for disclosure of certain attributes	3
Disclosure of unique identifiers	4
Prohibited marketing purposes	6
Prohibition on data profiling to track online behaviour	6
Retention	7
Prohibited retention of certain attributes	7
Destruction or de-identification	8
Personal information obtained through the Australian Government Digital ID System (AGDIS)	8
Personal information obtained through other digital ID systems	8
State and Territory privacy legislation	8

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.

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](#) (APP 3, APP 4, and APP 5) 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 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

Collection of this information is prohibited because it is not necessary information for verifying an individual's identity.¹

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.

An accredited entity 'solicits' an attribute of an individual if the accredited entity requests another entity to provide the attribute, or to provide information that includes the attribute.

¹ See [28] of the Revised Explanatory Memorandum to the Digital ID Act 2024.

The prohibition does not prevent other kinds of attributes of individuals being collected, even if a prohibited attribute can reasonably be inferred from those other permitted attributes. For example, an individual's name or place of birth are permitted attributes and can be collected by an accredited entity if it is reasonably necessary for their activities (see APP 3,) even if an individual's racial or ethnic origin can reasonably be inferred from that information

Use and Disclosure

An accredited entity must comply with [Australian Privacy Principles](#) (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 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 1 December 2024, 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 individual⁵
 - 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 party⁶ if the entity’s conditions on accreditation include an authorisation to disclose the restricted attribute to the relying party.

Disclosure of unique identifiers

In respect of its accredited services, where an accredited entity (“assigning entity”) has:

- a) assigned a unique identifier to an individual within Australia’s Digital ID System; and
- b) discloses that unique identifier to another accredited entity or to a 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.

The following disclosures are not permitted:⁷

- ✘ the assigning entity must not disclose the unique identifier to any other entity
- ✘ where an accredited entity has a unique identifier disclosed to them by the assigning entity, they must not disclose the unique identifier to any other entity.

However, these disclosure restrictions do not apply for the following purposes:

- ✔ 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 entity⁸;
- ✔ the unique identifier is disclosed to another entity if the other entity is facilitating access to the entity for whom the unique identifier was created⁹;
- ✔ 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 Territory¹⁰.

The disclosure limitations in section 47 for unique identifiers interacts with APP 9 as follows:

- If the assigning entity is a private sector accredited entity, APP 9 does not apply as that identifier is not a government related identifier.
- If the assigning entity is an agency (as defined in the Privacy Act), APP 9 does not apply as it applies only to organisations.

⁷ s 47 of the Digital ID Act.

⁸ s 47(5) of the Digital ID Act.

⁹ s 47(5) of the Digital ID Act.

¹⁰ 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](#).

- If the assigning entity is an agency (as defined in the Privacy Act) and it discloses a unique identifier to another accredited entity or relying party that is a private sector entity, then while APP 9 applies, that is overridden by s 47(3) which prohibits on-disclosure except for the purposes identified above.

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:¹¹

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
- ✘ 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:¹²

- ✘ 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

¹¹ s 55 of the Digital ID Act.

¹² s 53 of the Digital ID Act.

An accredited entity must not use or disclose personal information it holds about an individual, if the personal information is any of the following:¹²

- ✘ 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](#).

Retention

Prohibited retention of certain attributes

An accredited identity exchange provider must not retain the following attributes collected during an authenticated session¹³:

- 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.¹⁴

¹³ 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.

¹⁴ s 56 of the Digital ID Act.

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:¹⁵

- the personal information was obtained by the entity through AGDIS;
- the entity is not required or authorised by law¹⁶ 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.

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 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.

¹⁵ s 136 of the Digital ID Act.

¹⁶ This includes the Digital ID Act and related rules but excludes any prescribed laws.