



Australian Government

Office of the Australian Information Commissioner

Express consent in Australia's Digital ID System

Contents

Express consent obligations	1
Elements of express consent	2
Digital ID (AGDIS) Data Standards 2024	4
Capacity and accessibility requirements	5
Varying and withdrawing consent	5
Record keeping	5
Checklist	5



Express consent obligations

Under the *Digital ID Act 2024* (Digital ID Act), accredited entities are required to obtain express consent from individuals for many collections, uses and disclosures of their data. Express consent requirements form part of eight of the additional privacy safeguards (listed below).

Express consent provisions regulated by the Office of the Australian Information Commissioner

- ✓ Section 45: Individuals must expressly consent to disclosure of certain attributes to a relying party.
- ✓ Section 46: Accredited entities need express consent before disclosing a restricted attribute to a relying party.
- ✓ Sections 48, 49 and 50: In addition to the handling of biometric information only being permitted in specified authorised circumstances, accredited entities also require express consent to handle biometric information unless an exception applies. Exceptions include certain circumstances when disclosing biometric information to a law enforcement agency.
- ✓ Section 51: Express consent is required for biometric information of individuals to be retained for the purposes of further authenticating their digital ID.
- ✓ Section 54: Certain personal information must not be used or disclosed for prohibited enforcement purposes unless an exception such as the provision of express consent applies.
- ✓ Section 55: Individuals must expressly consent to the provision of marketing information.

Additional obligations relevant to consent are set out in the:

- *Digital ID (Accreditation) Rules 2024* (Accreditation Rules) (in particular, rules 4.40 – 4.41 relate to providing clear information about express consent and the duration of consent, rule 4.20 relates to logging requirements and recording consent in a transaction, and rule 7.1 which prescribes additional attributes that an accredited entity must obtain express consent for before disclosing).
- *Digital ID (AGDIS) Data Standards 2024* (AGDIS Data Standards) which are applicable to accredited entities approved by the Digital ID Regulator to provide accredited services in the AGDIS. In particular:
 - standards 2.2 – 2.3 of Schedule 1 which form part of role specific requirements for an accredited identity exchange provider,
 - standards 1.10 and 2.7.4 of Schedule 2 which form part of the requirements for the OpenID connect protocol (in the AGDIS context) for a participating

- accredited identity service provider to be able to facilitate secure Digital ID transactions, and
- standard 1.2 and Chapter 2 and Chapter 3 of Schedule 3 which outlines attribute sharing policies and how foundational attributes are used to identify individuals in the AGDIS.

Elements of express consent

Consent requires the following four elements:

1. The individual is adequately informed before providing consent.
2. The individual gives consent voluntarily¹.
3. The consent is current and specific.
4. The individual has the capacity to understand and communicate their consent.

The privacy safeguards in the Digital ID Act require accredited entities to obtain an individual's 'express consent'. This means that, in addition to the individual's consent meeting the above four elements, the individual must explicitly give their consent, such as by actively ticking a checkbox to indicate they consent. An accredited entity cannot infer or assume the individual has consented.

Example: MoneyCo Bank is a relying party and provides multiple options to facilitate access to their online banking services. Rachel is a MoneyCo Bank customer and chooses to access MoneyCo's online banking service using her digital ID with an accredited Identity Service Provider (ISP).

Rachel is redirected to their ISP for authentication and then to the accredited Identity Exchange Provider (IXP).

Under section 45 of the Digital ID Act, to authenticate Rachel's identity to the relying party, an accredited entity needs Rachel's express consent to disclose an attribute associated with her, or derived from another attribute to the relying party. Therefore, the IXP, as the conduit between the ISP and the relying party, must obtain Rachel's express consent for the disclosure to occur.

To do this, the IXP must meet the elements of express consent and comply with the additional specific obligations in the Accreditation Rules and any applicable data standards. For example:

¹ In the context of Digital ID, the concept of giving consent voluntarily can mean that subject to some exemptions, participating relying parties cannot require an individual to create or use a digital ID as a condition of accessing or providing a service (see s 74(1) of the Digital ID Act). This aligns with the [APP guidelines](#) which considers consent to be voluntary if, among other things, there are alternatives open to the individual should they choose not to consent.

- Adequately informed: the IXP must ensure that Rachel is properly and clearly informed about what personal information will be disclosed, for what purpose, how that information will be handled, and the implications of providing or withholding consent. This concept is also further reflected in part in Rule 4.40 of the Accreditation Rules, which requires an accredited entity to ensure the process and description for an individual to provide express consent is in clear, simple and accessible terms.
- Current: The IXP must ensure that it has a current consent from Rachel to disclose the information. Here, the IXP seeks a new express consent at the time Rachel is redirected to her IXP as part of her seeking to access her online banking service, so the consent is current. At the same time, the IXP also gives Rachel the opportunity to provide express consent for future disclosures to MoneyCo for Digital ID authentication purposes for 6 months, and Rachel grants this consent. In accordance with Rules 4.41(3)(c) of the Accreditation Rules, this ongoing consent will expire in 6 months as this was the consent period specified by the IXP when collecting the consent.
- Specific: the consent sought by the IXP should clearly and specifically describe what Rachel is being asked to consent to in terms of what information will be disclosed and for what purpose. For example, a request for specific express consent under section 45 should outline which attributes² are required and how they will be used. The IXP should not seek a broader consent than it needs in this situation (which is to handle Rachel's information for the purposes of authenticating her Digital ID). Ensuring the consent sought is 'specific' will also prevent 'bundled consent' which would occur where multiple requests for consent to a wide range of personal information handling were bundled together so that Rachel was unable to choose which collections, uses and disclosures she agrees to or not.
- Capacity: to provide consent, an individual must have the capacity to provide and communicate that consent. Generally, an accredited entity can assume an individual has capacity to consent, unless there is something to alert it otherwise, so in this example, the IXP may assume that Rachel has the capacity to provide express consent. Issues that could affect an individual's capacity to consent include physical

² Attributes contained in section 45 of the Digital ID Act are as follows:

- (a) the individual's current name or former name;
- (b) the individual's address;
- (c) the individual's date of birth;
- (d) the individual's phone number;
- (e) the individual's email address;
- (f) an attribute of a kind prescribed by the Digital ID (Accreditation) Rules (see rule 7.1).

or mental disability, temporary incapacity, or limited understanding of English.³ See below for a discussion of accessibility requirements that can assist in ensuring consent is properly obtained.

- Express consent: Rachel's consent must be given explicitly, rather than being inferred or assumed from the fact she is seeking to use the Digital ID option to access MoneyCo's online banking services. In this context, the IXP could ensure they obtain Rachel's express consent by requiring her to actively tick a checkbox or click a button to confirm consent is granted. The IXP should not rely on the failure to untick a pre-filled checkbox to establish that express consent has been granted.

Having met the consent requirements, the IXP has now obtained Rachel's express consent to the disclosure of her attributes to MoneyCo. The IXP can then create the session with MoneyCo and Rachel is able to use her online banking services by logging in with her Digital ID.

AGDIS Data Standards

If the accredited entity holds approval to provide a service within the AGDIS, the AGDIS Data Standards prescribe the 'consent type' the entity must use in different scenarios that requires consent. Accredited entities participating within the AGDIS must comply with the AGDIS Data Standards in addition to the Accreditation Rules, Accreditation Data Standards and Digital ID Rules.

The different 'consent types' identified in the AGDIS Data Standards are as follows:

1. Not required: express consent is not required for the attribute or attribute set.
2. Every use: express consent is required every time the attribute or attribute set is shared.
3. Ongoing: express consent is required at least the first time the attribute or attribute set is bound to the individual or shared.
4. Every change: express consent, for the attribute or attribute set, is required the first time the attribute or attribute set is shared with the participating relying party and every time it is modified.

For more information on consent types, refer to the AGDIS Data Standards 2024.⁴

The AGDIS Data Standards do not apply when accredited entities are providing accredited services outside of the AGDIS.

³ More generally, age is a factor that can affect an individual's capacity to consent. However, the Digital ID (Accreditation) Rules 2024 prohibit an ISP from generating a Digital ID for an individual less than 15 years old (rule 5.2), so an accredited entity can assume that an individual with a Digital ID can be presumed to be 15 years or older.

⁴ Refer to 1.2.1 of Schedule 3 of the Digital (AGDIS) Data Standards 2024

Capacity and accessibility requirements

Rule 4.49 of the Accreditation Rules requires accredited entities to meet a range of accessibility obligations. The intent of these obligations is to ensure individuals have access to clear, simple and easy to understand information about an entity's accredited services, and that those accredited services are accessible to individuals who experience barriers when creating or using a Digital ID.

Meeting these accessibility requirements in relation to the provision of accredited services may address some aspects of the capacity to give and communicate consent. Entities must take reasonable steps to ensure information is available in multiple accessible formats. For example, accessible formats may include screen-readable webpages and plain English or foreign translations ensuring individuals with vision impairment or limited English language skills can still provide informed consent.

Varying and withdrawing consent

An individual can vary or withdraw their consent at any time. Under Rule 4.40 of the Accreditation Rules, accredited entities must ensure the process and description of varying or withdrawing consent is explained in clear, simple and accessible terms.




Once an individual has withdrawn consent, entities are no longer allowed to rely on that past consent for any future use or disclosure of personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

Record keeping

Accredited entities should be aware of obligations in the Accreditation Rules for audit logs to be generated which include details of express consents obtained. For example, see rule 4.20(5)(h) of the Accreditation Rules.

Checklist

When entities are obtaining consent, they must implement procedures and systems which ensure that:

-  The process and description to inform individuals on the provision of consent is in clear, simple and accessible terms.
-  Relevant accessibility requirements are met.
-  The consent obtained is current and specific.

When entities are obtaining consent, they must implement procedures and systems which ensure that:

- ✓ Accurate records are generated and maintained that include details of express consents obtained.
- ✓ Individuals can vary or withdraw consent at any time and the process is easy and accessible.

When entities are obtaining consent, they should not:

- ✗ Rely on withdrawn or expired consent.
- ✗ Bundle consent.
- ✗ Seek broader consent than required.