Australian Government

Office of the Australian Information Commissioner

Handling biometric information when providing accredited Digital ID services

Contents

OAIC

Handling biometric information

An accredited entity is prohibited from handling biometric information, unless the handling is authorised under sections 49 or 50 of the *Digital ID Act 2024* (the Act). As part of an accredited entity's role, it may handle biometric information, but must ensure the proposed handling is authorised under one of these sections.

When would an accredited entity handle biometric information?

ID4U is an accredited identity service provider offering digital ID verification services. ID4U's accreditation conditions authorise ID4U to handle biometric information for the purposes of verifying the identity of an individual.

Lucy visits BanksRus' website to get a mortgage loan. BanksRus requires Lucy to verify her identity to proceed. BanksRus provides Lucy with multiple options (including Digital ID) for the verification process. Lucy decides to use a pre-existing IP2 level Digital ID, with ID4U, to verify her identity.

ID4U advises Lucy that BanksRus requires her to have an IP3 level Digital ID and she will need to provide photo ID so ID4U can carry out biometric matching to verify her for an IP3 level Digital ID. Lucy proceeds to upgrade her Digital ID to IP3 level by providing her photo ID for biometric matching. ID4U undertakes biometric matching and verifies Lucy's identity.

ID4U sends confirmation of Lucy's identity to BanksRus, and the mortgage loan is approved.

Now that the identity verification check is complete, ID4U deletes the biometric information immediately, or if required, retains the biometric information for no longer than 14 days for testing or fraud purposes.

In addition to complying with any accreditation conditions, an accredited entity must comply with their privacy obligations when handling biometric information in Australia's Digital ID System.

These privacy obligations include the Australian Privacy Principles (APPs) or applicable State or Territory privacy principles, and the additional privacy safeguards in sections 48 – 51 of the Act. Section 52 of the Act also states that the Accreditation Rules may provide for requirements in relation to the handling of biometric information, such as requirements in relation to quality, security or fraud.[1]

Different obligations apply to the handling of personal information that is not biometric information, and these are addressed separately in guidance on Handling personal information when providing accredited Digital ID services.

[1] Rules 2.3(3)(e), 4.7(3), 4.12(5), (6) and (7) in the Digital ID (Accreditation) Rules are examples of rules in relation to biometric information.

What is biometric information?

'Biometric information' of an individual is information about any measurable biological characteristic relating to that individual that could be used to identify them or verify their identity. This includes 'biometric templates'.

Biometric information can include any features of a person's face, fingerprints, iris, palm, signature, or voice. A biometric template is a digital or mathematical representation of an individual's biometric.[2]

Handling biometric information with an individual's express consent

The permitted circumstances where an accredited entity can handle biometric information with an individual's express consent are listed below:

Permitted handling of biometric information with express consent
• Conditions on accreditation authorise the collection, use or disclosure of the individual's biometric information and it is being handled for the purposes of the accredited entity doing either or both of the following: o verifying the identity of the individual o authenticating the individual to their Digital ID[3]
• Disclosure to a law enforcement agency for the purposes of: o verifying the identity of an individual, or o investigating or prosecuting an offence[4]
• Collection, use, disclosure or retention of biometric information for the purposes of issuing a government identity document or credential[5]

Handling biometric information without an individual's express consent

There are circumstances where an accredited entity is authorised by section 49 of the Act to handle biometric information of an individual without that individual's express consent. These permitted circumstances are listed below:

[2] GPA Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology.

[3] s 49(1) of the Digital ID Act.

[4] s 49(3)(b) of the Digital ID Act.

[5] s 50 of the Digital ID Act for further information on those entities covered by this section.

Permitted handling of biometric information without express consent
Disclosure to a law enforcement agency is required or authorised by or under a warrant[6]
Disclosure is to the individual to whom the biometric information relates[7]
Retention, use or disclosure is for undertaking testing in relation to the biometric information[8]
Retention, use or disclosure is for preventing or investigating a digital ID fraud incident[9]

Prohibited handling of biometric information

An accredited entity is prohibited from collecting, using, disclosing or retaining biometric information of an individual in Australia's Digital ID System, unless it is specifically authorised under sections 49 or 50 of the Act.[10]

The Act also specifically prohibits the collection, use or disclosure of biometric information for the following two purposes:

- one-to-many matching of the individual
- determining whether the individual has multiple Digital IDs.[11]

What is one-to-many matching?

One-to-many matching is also known as biometric identification matching. This process refers to comparing a biometric template of an individual against all other biometric templates in a system, generally to identify the individual. Collecting, using or disclosing biometric information for one-to-many matching is prohibited under the Act.[12]

[6] s 49(3)(a) of the Digital ID Act.

[7] s 49(5) of the Digital ID Act.

[8] s 49(6) of the Digital ID Act – the accredited entity must have collected the information in accordance with subsection 49(1) and the entity complies with any requirements prescribed by the Digital ID (Accreditation) Rules. The accredited entity must take reasonable steps to continuously improve its biometric systems to ensure such systems do not selectively disadvantage or discriminate against any group.

[9] s 49(8) of the Digital ID Act – the accredited entity must have collected the information in accordance with subsection 49(1) and the entity complies with any requirements prescribed by the Digital ID (Accreditation) Rules.

[10] s 48 of the Digital ID Act.

[11] s 48(3) of the Digital ID Act.

[12] s 48(4) of the Digital ID Act.

This is opposed to one-to-one matching also known as biometric verification matching. This process refers to matching a biometric template of an individual with a single stored biometric template to verify the identity of the user. This process answers the question 'is the user who they claim to be?'.[13] For the situations in which the handling of biometric information is authorised under section 49 or 50, many of these situations require the accredited entity to also obtain the individual's express consent for the handling of the biometric information.

Destruction of biometric information

An accredited entity that handles biometric information must comply with the destruction requirements set out in the Act. Destruction requirements vary depending on the accredited entity's purpose for handling the biometric information.

Collection was for the purposes of verifying an individual's identity only[14]

Must be destroyed immediately after the verification is complete.

Collection was for the purposes of authenticating the individual to their Digital ID

- Must be destroyed immediately after the authentication is complete (unless the individual has given express consent for that information to be retained for the purposes of further authenticating).[15]
- Must be destroyed immediately after an individual withdraws their consent for the biometric information to be retained for the purposes of authenticating.[16]

Retention was for the purposes of testing

Must destroy the information at the earlier of:

(a) the completion of testing the information; and

[13] For privacy guidance on facial recognition technology, refer to OAIC's 'Facial Recognition Technology: a guide to assessing the privacy risks' document.

[14] s 51(1) of the Digital ID Act.

[15] s 51(2) of the Digital ID Act.

[16] s 51(3) of the Digital ID Act.

(b) 14 days after the entity collects the information.[17]

Retention was for the purposes of activities relating to the prevention or investigation of the digital ID fraud incident

Must destroy the information at the earlier of:

(a) immediately after the completion of activities relating to the prevention or investigation of the digital ID fraud incident (as the case may be); and

(b) 14 days after the entity collects the information.[18]

[17] s 51(4) of the Digital ID Act.

[18] s 51(5) of the Digital ID Act.