Australian Government | Digital Identity

Digital Identity Legislation Position Paper

Summary

The need for Digital Identity legislation

The government is committed to rolling out a whole-of-economy digital identity system to include state, territory and local government, as well as the private sector.

The purpose of the legislation is to:

- allow for independent oversight of the system, by formalising the powers and governance arrangements of the Independent Oversight Authority
- enable the system to expand to state, territory and local governments and the private sector
- ensure privacy protections and consumer safeguards to build trust in the system
- provide a legally enforceable set of rules that set the standards for participating in the Digital Identity system, including for accreditation
- allow for entities to be accredited for their activities whether they are connected to the Commonwealth's Digital Identity system or not.

About the Digital Identity Legislation Position Paper

There are 8 key positions covered in the paper that aim to achieve the intended purpose of the legislation.

01 Structure of the Digital Identity legislation

02 Scope of the Digital Identity legislation and interoperability with other systems

03 Governance of the Digital Identity system

04 Privacy and consumer safeguards

05 Trustmark(s)

06 Liability and redress framework

07 Penalties and enforcement

08 Administration of charges for the Digital Identity system

Digital Identity Legislation Position Paper summary

01 The structure of the legislation

The legislation will consist of:

- primary legislation with important privacy and consumer safeguards
- rules and policies, including accreditation standards.

Refer to section 4 of the Position Paper.

02 The scope of the legislation and interoperability with other systems

The legislation will have a clearly defined scope:

- legislation will not limit a person to having one digital identity with one provider
- legislation is not intended to regulate all digital identities and digital identity systems
- entities decide whether they will use the system or provide services on the system
- legislation will leverage existing laws, not duplicate them
- relying parties will need to offer a choice of identity providers
- entities generating, transmitting, managing, using and reusing digital identities will need to provide a seamless user experience with the Digital Identity system (interoperability).

Refer to section 5 of the Position Paper.

03 System governance

The legislation will set the governance arrangements for the system allowing for:

- the Minister to appoint a permanent Independent Oversight Authority
- effective and permanent governance arrangements that enforce consumer safeguards and provide confidence that privacy and security is protected, and enforced by law
- rules to be enforced by the Oversight Authority and Information Commissioner.

Refer to section 6 of the Position Paper.

04 Privacy and consumer safeguards

The legislation aims to include privacy and consumer safeguards that will:

- protect personal information and ensure accessibility for people with disabilities, those with limited access to technology, older Australians, and culturally and linguistically diverse Australians
- prohibit the creation of a single identifier used across the system and all government services
- require individuals to expressly consent before their attributes are shared with a relying party
- create a voluntary system giving users the right to create and use a digital identity, including the right to deregister and not use a digital identity at any time
- require relying parties to provide an alternative channel to digital identity for Australians to access their services. Exemptions will apply for small and other types of businesses.

Safeguards and biometric information

- Limit the system to one-to-one biometric matching only.
- Prohibit anyone other than those involved in proofing or authentication from collecting or using biometric Information.
- Prevent biometric information being sent to third parties not required to perform or proofing or authenticate a person.
- Require biometric information to be deleted once it has been used for its intended purpose.
- Allow users to consent to their biometric information being accessed for fraud or security investigations.

Restrictions on data profiling

- Prohibit the collection, use and disclosure of information about a user's behaviour on the system except to verify their identity, assist them to receive a digital service, allow them to view their own behaviour (for example, a dashboard) or support identity fraud management.
- Enforce record-keeping of metadata and activity logs for a minimum 7 years to maintain the system's integrity, and to allow for fraud or criminal investigations.
- Default minimum age of 15 years for the use of a digital identity.

Refer to section 7 of the Position Paper.

05 Trustmark(s)

The legislation will establish a trustmark (or trustmarks) to:

- help consumers identify when they are creating or using a digital identity in the system
- indicate to consumers that the services provided by an accredited participant has been accredited and meets Australian Government minimum standards.

Refer to section 8 of the Position Paper.

06 Liability and redress framework

The legislation will include a liability and redress framework to:

- govern how losses or damage suffered by those using the system will be managed
- involve mechanisms for non-financial redress for adverse outcomes that arise from participation in the system and management of financial liability, including the Oversight Authority and its staff
- ensure that accredited participants are not liable for loss or damage suffered provided they were acting in good faith, and complied with the legislative rules and requirements relating to the system
- establish a mechanism available to users affected by a cyber security incident, identity theft, inappropriate disclosure of information or system failure.

Refer to section 9 of the Position Paper.

07 Penalties and enforcement

The legislation will include a penalties and enforcement regime that will:

- allow entities to be penalised if they do not comply with the legislation and rules
- provide fair and proportionate penalties to the harm caused
- establish civil penalties for breaches of privacy safeguards, including unrelated marketing, biometrics and user consent
- enable the Oversight Authority to suspend or revoke accreditation and access to the system, and issue directions for remedial action to address a breach.

Refer to section 10 of the Position Paper.

08 Administration of charges for the Digital Identity system

The legislation aims to establish the following charging principles:

- charging to be fair and transparent, incentivising adoption and fostering inclusion
- charging relying parties for using the Digital Identity system
- the Government will not seek to recoup the costs of building the Digital Identity system
- the specific charging amount and/or charging formulas will be detailed in secondary legislation.

Refer to section 11 of the Position Paper.

Security requirements

The Digital Identity legislation will establish security requirements that will:

- continue to ensure high security standards with end-to-end cyber security and risk assessments
- provide the Oversight Authority with powers to coordinate the sharing of information between participants to support the management of cyber security and fraud incidents.

Refer to section 3.5.1 of the Position Paper.

Have your say

Your feedback on the Digital Identity Legislation Position Paper will help guide the development of the Digital Identity legislation. You can have your say by submitting your views on digitalidentity.gov.au before 5:00 pm AEST on 14 July 2021.