16 July 2021

CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

Digital Transformation Agency
PO Box 457
Canberra City
ACT 2601

By email: digitalidentity@dta.gov.au

Dear Sir / Madam,

Submission on the Australian Government's Digital Identity Legislation Position Paper

CPA Australia represents the diverse interests of more than 168,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

CPA Australia supports policy initiatives that make it easier for the community to interact with government. This includes making it easier for intermediaries such as accountants to engage with government on behalf of the clients they represent. However, such policies need to be balanced by appropriate standards of data privacy and security, and investment in suitable technologies to support both.

CPA Australia offers the following observations on the Position Paper:

Scope of the legislation and interoperability with other systems

With regards to the scope of the Digital Identity system, the Position Paper states that the legislation will allow the Digital Identity system to be expanded to the private sector and state, territory and local governments. We encourage the government to elaborate on how and for what purposes private sector institutions and territory and local governments will use the Digital Identity system.

While we believe that it is useful for those parties, including intermediaries such as accountants to use the system for verification purposes, we are not convinced of the need for them to directly access and/or hold Digital Identity information. Therefore, we recommend that the purposes for which private sector institutions and territory and local government entities will have access to and use the system be narrowly defined.

Privacy and consumer safeguards

We encourage the government to outline in greater detail:

- how it intends to assure that biometric data is used for intended purposes only, and
- what safeguards it will implement to provide data access to authorised parties only.

We consider the deletion of biometric information – after using it for intended purposes – as crucial. The government should clarify whether such information is deleted from the database only or is entirely removed from the servers/location where the information is stored.

Further, we note that users will have the right to deregister their Digital Identity and not use a Digital Identity at any time. While we agree with these proposals, we suggest that the government clarifies what happens to the user's data once a user has executed the right to deregister.

Accreditation and trustmark(s)

While the accreditation process appears to be fit for purpose, we believe further elaboration is needed on how the proposed Oversight Authority intends to manage the process of revoking accreditation. This includes cases where accredited participants, including government entities, fail to comply with the rules and standards of the Digital Identity system. In stating this, we acknowledge that withdrawing accreditation from government entities may pose significant challenges for the provision of public services that require identity verification.

With regards to the accreditation process, we emphasise that it is crucial for entities to outline in detail for which role(s) they are seeking accreditation. This mitigates the risk of trustmarks being used by accredited entities for other purposes.

Penalties and enforcement

We encourage the government to consider adding criminal penalties to civil penalties for serious willful breaches of privacy. We believe that there should be significant consequences for those who breach this right.

Administration of charges for the Digital Identity system

We do not support there being a cost for using the Digital Identity system – we see it as a public good that will benefit society and the economy.

We are aware of the costs of the existing Document Verification Services (DVS). The problem we identify is that government or private sector institutions using the system may pass their costs to citizens and residents, who should not be charged for proving their identity.

Oversight Authority

As the statutory officeholder responsible for the administration and oversight of the Digital Identity system and for the accreditation of entities, the Oversight Authority will play an important role. We note that the Oversight Authority can be supported by the entity best equipped to do the job. We encourage the government to address the following questions in detail:

- how is "the job" defined and what does it entail?
- what criteria will be used to determine which entity is "best equipped"?

Other observation

The proposed design should support the expansion of the regtech sector (i.e. intermediaries like DVS). It should also seek to eliminate the need for government and other third parties to authenticate individuals by, for example, checking myGovID credentials. This reduces the costs on society, reduces risk and is more efficient.

If you have any questions about this submission, please do not hesitate to contact Dr. Jana Schmitz, Technical Advisor, Assurance and Emerging Technologies at CPA Australia on jana.schmitz@cpaaustralia.com.au.

Yours sincerely

Dr Gary Pflugrath CPA
Executive General Manager, Policy and Advocacy