information and privacy commission
new south wales

Enquiries: [redacted]
Telephone: [redacted]
Our reference: IPC20/A000509

10 December 2020

Digital Transformation Agency
PO Box 457
Canberra City ACT 2601

Submitted via www.digital.identity.gov.au

Dear Sir/Madam

DIGITAL IDENTITY LEGISLATION CONSULTATION PAPER

This is a submission to the Digital Identity Legislation Consultation Paper released by the Australian Government's Digital Transformation Agency. This submission provides general commentary and specific responses to identified proposals and questions contained within the Consultation Paper.

The NSW Privacy Commissioner administers the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) and promotes awareness and understanding of privacy rights in NSW. The PPIP Act and HRIP Act establish the Information Protection Principles and Health Privacy Principles which govern the collection, security, use and disclosure of personal and health information by NSW government agencies and, in the case of the HRIP Act, private sector health care providers.

Privacy safeguards

Appropriate privacy and consumer protections are an essential requirement for building public trust in the digital identity system. To that end, the primary legislation should contain strong privacy and consumer protections. These should, at a minimum, be consistent with the privacy requirements under the current Trusted Digital Identity Framework (TDIF) and include:

- ensuring that use of Digital Identity is voluntary
- a prohibition on the commercialisation of personal information obtained via the Digital Identity system and the profiling of individuals
- a restriction on the creation and use of a single identifier for the entire system
- restricting the use and retention of biometric information to those required for verification on the system
- requiring express consent from an individual or their authorised representative to use the system to authenticate and pass attributes to a service.

Interaction with state & territory laws

The legislation should include provisions which detail how it will interact with relevant state and territory laws. This will include privacy legislation, information access legislation and state record legislation.

Consent

It is appropriate that the legislation embed a requirement for the user to consent before transacting with a relying party and that this occur each time the person transacts with a relying party. A specific mechanism enabling an individual to opt-out of the system after they have created a Digital Identity should also be included in the legislation.

The consultation paper indicates that where a person opts-out, the system will retain information from the discontinued Digital Identity for purposes such as fraud investigation. Consideration should be given to the addition of a time limit for which such information may be retained.

It is appropriate that the legislation include a prohibition on requiring someone to use digital identity. This lack of compulsion is central to ensuring that individuals can freely give consent and that obtaining a Digital Identity remains voluntary.

Digital discrimination

As more services are subject to digitisation, care should be taken to ensure that citizens who are unable to transact digitally are not disadvantaged or discriminated against. This is a significant risk for individuals from marginalised and economically disadvantaged communities.

The legislation should require participating organisations to provide an alternative non-digital channel of identity verification for individuals who are unable to access, or choose not to access, digital identity systems. These individuals should not be locked out of access to services that are accessible to other citizens.

Definition of 'digital identity information'

The legislation should include clear a definition of what is digital identity information.

The legislation should confirm that all data collected, stored and used by Identity Providers is personal information under the *Privacy Act 1988* (Cth) (Privacy Act). Additionally, the legislation should also provide that the meta-data held by the Identity Exchange should always be treated as if it was personal information within the meaning of the Privacy Act.

Use – restrictions on secondary use

The legislation should provide clear provisions on how digital identity information may be used. It is noted that the use of personal data for direct marketing is completely prohibited in the TDIF Privacy Requirements (section 2.6). This requirement should be replicated within the legislation.

Biometrics

The limitations on the use of biometric information proposed in the consultation paper are appropriate given the sensitive nature of this information.

The legislation should include express prohibitions on the use of biometric information for any purpose other than those expressly established by the legislation, and the disclosure of biometric information to a third party. Additionally, the legislation should include an obligation to destroy all biometric information once the verification process has concluded except in the limited circumstances outlined in the consultation paper.

Privacy law coverage

The consultation paper indicates that the legislation will allow state and territory agencies to participate in the system where they are subject to legislation that offers equivalent levels of privacy protection to the Privacy Act. I note that there has been no consultation with the Information and Privacy Commission NSW to date on what equivalency might mean in the context of the Digital Identity system and I look forward to this consultation.

The consultation paper also notes that some Accredited Participants under the system may fall outside of the coverage of the Privacy Act. This should be addressed in the primary legislation with small business required to opt-in to the Privacy Act under section 6EA of that legislation.

Privacy Impact Assessment

The requirement under the current TDIF accreditation that all participants undertake a privacy impact assessment should be replicated in either the primary legislation of the operating rules. A privacy impact assessment (PIA) is an important 'privacy by design' process, ensuring that privacy considerations are built into a project from conception through to implementation.

The benefits of the PIA process include:

- enabling early identification of adverse privacy impacts and an opportunity to address these
- promoting awareness of privacy issues and building privacy risk management capacity in an organisation
- complying with privacy laws
- demonstrating that privacy is a core corporate value and that a project is designed with privacy and privacy safeguards in mind
- building good will, trust and confidence of the community and stakeholders that a project is privacy compliant.

I hope that these comments will be of assistance in your consideration of this matter. Please do not hesitate to contact me if you have any queries. Alternatively, you may contact [redacted], [redacted], on [redacted] or by email at [redacted].

Yours sincerely

[redacted]

Samantha Gavel
Privacy Commissioner