Digital Identity Legislation Exposure Draft
Digital Transformation Agency (D.T.A)

via email: digitalidentity@dta.gov.au

27th October 2021

Submission on Digital Identity Legislation Exposure Draft 2021 to the Digital Transformation Agency

P.w.C welcomes the release of the **Digital Identity Legislation Exposure Draft** and believes it is an important step in supporting Australia in the continued development of enabling components for the digital economy such as an Australian digital identity ecosystem. Over the last twelve months, PwC has been involved in the public consultation process that the D.T.A has undertaken and continues to support the progress made in developing the governance functions and principles outlined in the legislation.

As one of Australia's leading professional services firms, with touch points across the Digital Trust system, we have unique perspectives that we can share on these important issues as this legislation draft goes through its final phase of public consultation. This submission paper for phase 3 of the consultation process includes points of view on the upcoming draft legislation, Trusted Digital Identity Framework (T.D.I.F) Accreditation Rules and Trusted Digital Identity (T.D.I) Rules which we feel we are well positioned to contribute to, based on our experience and insights from both clients and colleagues across our global network.

Overall, the draft legislation, T.D.I.F Accreditation Rules and T.D.I rules appear to have incorporated much of the feedback shared over the consultation period and are in line with the direction outlined by the Government. We believe there are some opportunities for improvements that would greatly assist with the smooth and timely implementation of the legislation. As such we have outlined some observations and recommendations as an attachment which we hope can improve clarity around some aspects of the legislation to enable a fast paced and high quality implementation. We would welcome the opportunity to discuss our views further. Please feel free to contact me directly on the contact details below.

Kind regards

Mary Attard
Partner, Cyber Security and Digital Trust
PwC Australia
Email: mary.attard@pwc.com

Attachment

Privacy Act / Bill interaction:

PwC welcomes the innovative approach to leveraging the existing Notifiable Data Breach scheme in Part IIIC of the *Privacy Act 1988* (Cth) (**Privacy Act**) and extending the definition of personal information under the Privacy Act to include attributes, restricted attributes and biometric information (as defined in the Bill) rather than developing a new customised incident reporting regime in respect of the unauthorised disclosure of personal information by onboarded entities.

The latter approach would have likely resulted in onboarded entities having to comply with duplicative notification requirements and managing parallel regulatory investigations as well as a broader risk that they could incur a penalty from both the Information Commissioner and the Oversight Authority for the same data breach. The approach proposed in the legislation (including by authorising the Information Commissioner to enforce the penalties for any breach of the 'additional privacy safeguards' in Division 2 of Part 4) will allow participants to benefit from the Information Commissioner's extensive experience in investigating incidents and data breaches.

Although the Notifiable Data Breach Scheme will largely govern the system in respect of incidents, PwC notes that the Oversight Authority will operate a 'scaled-down' incident notification regime in parallel as the legislation contemplates a concept of 'reportable incidents' which include, amongst other things, digital identity fraud incidents and cyber security incidents (which do not have to involve the disclosure of personal information in order to be reportable).

Under s10 of the Trust Digital Identity Rules, any entity that suffers a reportable incident must notify the Oversight Authority and any entity that suffers a cyber security incident or a digital fraud incident must make all reasonable efforts to contact any individuals affected by the incident and any business acting on behalf of that individual. This is understandable as the Oversight Authority should retain a notification obligation in respect of incidents that don't meet the '*serious harm*' threshold under the Notifiable Data Breach Scheme.

However, in view of the 'fast-moving' nature of cyber incidents the Oversight Authority can consider further ways to streamline the management of reportable incidents for onboarded entities. For example, onboarded entities could be exempt from notifying the Oversight Authority in accordance with the legislation if they can demonstrate that the reportable incident has or will be reported to the Information Commissioner under the Notifiable Data Breach Scheme.

Similarly, onboarded entities could have a right to notify the Oversight Authority that the notice to affected individuals required under s43, will separately be provided under s26WL of the Privacy Act and in accordance with those more generous timeframes, thus giving onboarded entities more time to collate an appropriate notice and obtain the full detail of the relevant reportable incident rather than providing separate notices to individuals under regime.

P.w.C sees the potential in the collaboration between the Information Commissioner and the Oversight Authority in undertaking the joint administration of the legislation. However, in pursuing a joint regulatory model, we believe that consideration should be given to how this will work in practice. We note that the onus is on onboarded entities to provide the Oversight Authority with a copy of any data breach notification provided to the Information Commissioner under the Privacy Act (or where any participant is bound by any equivalent state/territory data breach regime, a copy of any data breach notification provided to that privacy authority). Presumably, for this to be effective, the two regulators will need to consult and share information in order to discharge their own regulatory responsibilities and this is contemplated by s70 and 71 which allows the Information Commissioner to disclose the details of any investigations to the Oversight Authority.

As the Information Commissioner will be the ultimate decision-maker in respect of a data breach (unlike the Financial Accountability Regime Bill 2021 (F.A.R) which also adopts a joint regulatory model but allows A.P.R.A and A.S.I.C to make decisions separately) the role and power of the Oversight Authority will need to be clearly agreed in intragovernmental arrangements and this will need to be in place at the commencement of the Act. Onboarded entities will expect cohesion and consistency in their communications with both regulators and it is therefore important that the Oversight Authority and the Information Commissioner are aligned on key principles prior to the implementation of the new system.

T.D.I.F vs T.D.I Rules

A resilient digital identity ecosystem is one that strikes the right balance between legislatively enshrined principles and adaptive, agile technical guidance. The Trusted Digital Identity Framework (T.D.I.F) has served the D.T.A and the wider ecosystem well as a technical guiding framework incorporating changing international standards and responding to the needs of ecosystem participants, while remaining free from the complex and slow-moving processes of official legislation.

These advantages are due to change as the T.D.I.F is replaced by the *T.D.I and T.D.I.F Accreditation Rules* which will require Parliamentary approval to be actively managed and updated. As per P.w.C's response to the digital identity legislation position paper submitted in July 2021, our experience in digital identity management indicates that for an ecosystem to remain resilient and able to proactively address changes in best practices the D.T.A should consider what mechanisms can be established to trigger reviews and updates to this technical guidance and the degree to which legislative enshrinement may impede this active management.

Multiple Ecosystems

As digital identity in Australia matures, multiple ecosystems will emerge introducing greater complexity. These emerging ecosystems will likely represent a wide range of industries and levels of government with various competing use cases and goals for participation in Digital Identity. It is likely that the Australian digital identity landscape will soon be composed of a range of accredited and non-accredited participants, with various degrees of required compliance to the proposed Bill.

As per P.w.C's response to the digital identity legislation position paper submitted in July 2021, the proposed governance arrangement will need to consider how it will accommodate different models of identity from these various emerging participants seeking to interface with the official government ecosystem. However, it remains unclear how the current proposed governance arrangement will facilitate interoperability and manage the additional fraud, privacy, accessibility and trust implications brought about by multiple ecosystems.

This multi-ecosystem governance function is important given the potential range of competing priorities that participants will have to traverse, such as the strict A.M.L/C.T.F regulation and critical infrastructure obligations for financial sector participants which may have unintended impacts on responsiveness and resilience of the core digital identity system.