13 July 2021

Digital Transformation Agency
PO Box 457
Canberra City ACT 2601

Via electronic submission – digitalidentity.gov.au

DIGITAL IDENTITY CONSULTATION – PHASE 2

Amazon Web Services, Inc. (AWS) appreciates the opportunity to contribute to the second phase of the Digital Transformation Agency's (DTA) consultation on Australia's Digital Identity legislation. Customer trust and security are core to AWS's operations and services, and we welcome the Australian Government's commitment to a whole-of-economy Digital Identity system.

For over 15 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 81 Availability Zones (AZs) within 25 geographic regions, with announced plans for 21 more Availability Zones and seven more AWS Regions including Melbourne. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs.

Scope of the legislation

AWS's understanding from the position paper is it is intended that the Trusted Digital Identity Framework (TDIF) and Legislation would apply to accredited TDIF participants (attribute service providers, identity providers, credential service providers, or identity exchanges), but not extend to service providers that these accredited participants may use, including digital, data, and cloud service providers.

This distinction is important, particularly when seeking to legislate a framework for a digital solution. Cloud service providers (CSPs) are responsible for security 'of' the cloud - the hardware, software, networking, and facilities that run the cloud services. However, CSP customers are responsible for the security of their data and applications 'in' the cloud, utilising the comprehensive suite of tools and controls available. CSPs do not typically have access to or visibility of customers' data that is stored or processed on their infrastructure.

AWS recommends that the explanatory memorandum and legislation should make clear that the direct providers that are included in the scope of the legislation are limited to entities who choose to participate in the scheme, and are authorised to access and use data as part of the scheme. The explanatory memorandum

and legislation should also make clear that the providers of underlying technology services are not captured and impacted. Where a participant engages a technology service provider to hold and process data on instructions from a scheme participant, the scheme participant should not be considered to share the data with the service provider, and the service provider should not need to participate in the scheme.

AWS appreciates the opportunity to make this submission and would be pleased to provide the DTA further information or support in its consideration of the Digital Identity legislation.

Yours sincerely,

Roger Somerville (somroger@amazon.com)
Head of Public Policy, Australia and New Zealand
Amazon Web Services