10 October 2023

BSA & GDA COMMENTS ON THE DIGITAL IDENTITY DRAFT LEGISLATION

Submitted Electronically to the Department of Finance

BSA | The Software Alliance (**BSA**)[1] and the Global Data Alliance (**GDA**)[2] welcome the opportunity to submit comments to Australia's Department of Finance on its draft Digital Identity Bill 2023 (**Digital ID Bill**) and the accompanying draft Digital Identity Rules 2024 (**Digital ID Rules**).[3] We welcome the Government's efforts to develop legislation for an economy-wide Digital ID system. We note that one of the draft legislation's policy objectives is to ensure that accredited Digital ID providers keep personal information private and secure.[4] Indeed, while digital IDs offer substantial convenience and efficiency, robust privacy protections are necessary to mitigate risks of unauthorised access and misuse of personal information.

In this regard, BSA and GDA would like to register our concerns with paragraph 73 of the Digital ID Bill and paragraph 10 of the Digital ID rules. Paragraph 73 of the Digital ID Bill will allow the Government to set rules pertaining to "the holding, storing, handling or transfer of information outside Australia if the information is or was generated, collected, held or stored by accredited entities within the Australian Government Digital ID system"; as well as to "prohibit…the holding, storing, handling or transferring of such information outside Australia". Paragraph 10 of the Digital ID Rules stipulate that an accredited entity participating in the Australian Government Digital ID system "must not… (a) hold, store or handle system information at a place outside Australia; or (b) transfer system information to a place outside Australia for storage or handling" unless the entity holds an exemption granted by the Minister.

In essence, these provisions impose data localisation requirements on any entity which wants to obtain accreditation under the Australian Government Digital ID system. Governments often impose these requirements under the belief that storing data within a country's borders would

[1] BSA is the leading advocate for the global enterprise software industry, and our members develop cloud-enabled and data-driven services that help to create jobs and grow the digital economy. BSA members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. The GDA supports policies that help instil trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security, innovation, economic development, and international trade.

[3] Exposure draft of Digital ID Bill, September 2023, https://www.digitalidentity.gov.au/sites/default/files/2023-09/Exposure%20draft%20of%20the%20Digital%20ID%20Bill%202023.pdf. Exposure draft of Digital ID Rules 2024, September 2023, https://www.digitalidentity.gov.au/sites/default/files/2023-09/draft%20Digital%20ID%20Rules%20September%202023_0.pdf,

[4] Digital ID Bill consultation page, accessed October 2023, https://www.digitalidentity.gov.au/have-your-say.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

enhance privacy and cybersecurity. However, the security of data does not depend on where it is stored. In fact, requiring businesses to localise the data can undermine security by increasing risks and decreasing resilience.

For example, due to data localisation requirements, digital ID service providers may not have access to data storage and cybersecurity solutions provided by international cloud service providers. Local cloud service providers do not have the same security capabilities as their global counterparts, which benefit from collecting and processing security data[5] worldwide for security research, real-time threat monitoring and analysis of malicious cyber activities across regions and customers. This comprehensive approach is crucial for detecting and pre-empting potential cyber threats effectively, as well as developing mitigations to protect governments, businesses, and individuals around the world from attack. Without access to global data storage and cybersecurity solutions, the security capabilities of digital ID service providers will be more limited, which will ultimately compromise the privacy and security of users of the digital ID system.

Furthermore, requiring data to stay within a country would prevent a digital ID service provider from backing up data in offshore data centers to ensure redundancy. In case of a serious cyberattack or physical disruption, including natural disasters, data stored in a physically remote data center can be used to recover from the incident. The inability to create backups outside of country will adverse impacting resiliency.

Localisation measures are not also necessary for regulatory oversight, even in heavily regulated sectors such as the financial services sector. As a general principle, there is no reason to impose localisation requirements on businesses if regulatory authorities have immediate and ongoing access to data. In this regard, we note that Australia's Digital Trade Strategy[6] expressly acknowledges the importance of facilitating cross-border data transfers and prohibiting data localisation requirements. As the Digital Trade Strategy notes, "[u]nnecessary restriction on the flow of data, or requirements to store data locally raises costs for businesses and significantly reduces efficiencies, impacts the ability to make decisions on business development, marketing, innovation and development of comparative advantage, and makes it difficult for businesses to enter new markets".[7] We are also fully supportive of the approaches taken in Australia's Digital Economy Agreement with Singapore and the Australia-UK Free Trade Agreement, both of which set out binding rules prohibiting unwarranted restrictions on cross-border data transfers and requirements to localise computing facilities.

More recently, the Government's response to the Privacy Act Review Report[8] affirmed that "free flow of information is an increasingly important component of international trade and digital service modes", and is working to "support the free flow of information with appropriate protections".[9] In this vein, processing information overseas should be allowed so long as the risks are mitigated and appropriate safeguards are in place (e.g., the data processor receiving the data from Australia should be certified under a scheme that is deemed to provide substantially similar protection to the Australian Privacy Principles).

In the circumstances, we urge the Department of Finance to remove the imposition of data localisation measures set out in paragraph 73 of the Digital ID Bill and paragraph 10 of the Digital ID Rules. This would reassure the industry that Australia will not prohibit or restrict

---

[5] Security data can include device and network information, as well as other information such as URLs/domains, session data, threat intelligence or data, statistics, aggregated data, netflow data and "telemetry data".

[6] Digital Trade Strategy, April 2022, https://www.dfat.gov.au/sites/default/files/digital-trade-strategy.pdf.

[7] Digital Trade Strategy (2022), p. 10.

[8] Government Response to Privacy Act Review Report, September 2023, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

[9] Government Response to Privacy Act Review Report (2023), p. 16.

cross-border data transfers, which are crucial for both security and privacy. In addition to the above concerns, the Department of Finance should also consider how Part 4 of the Digital ID rules, which establishes a cybersecurity reporting regime, may undermine cybersecurity by adding additional complexity, as well as how its policy objective might be furthered by incentivising the adoption of key cybersecurity principles across all digital ID providers.

We hope that our comments will be taken into consideration as the Department of Finance moves forward with the Digital ID regulations. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong

Manager, Policy – APAC