TELSTRA GROUP LIMITED

Department of Finance

Digital Identity Legislation – Exposure Draft Consultation

Public submission

13 October 2023

01 Introduction

Telstra welcomes the opportunity to respond to the Department of Finance's exposure draft of the DI legislation. We commend the Department on a robust draft Bill that improves privacy, security, fraud prevention, user experience and inclusion.

Our submission provides feedback to the Department on matters we consider would benefit from additional clarity either in the *Digital Identity Bill 2023* (**the Bill**) or in the draft *Digital ID Rules 2024* (**Digital ID Rules**) and *Digital ID Accreditation Rules 2024* (**Accreditation Rules**) accompanying the main instrument. Our recommendations focus on matters we consider would assist with the commercial viability and uptake of the AGDIS System while balancing the trust and security requirements of the overall framework.

02 Liability framework should appropriately share risk between accredited entities and Government

2.1. Accredited entities need appropriate liability protections

As identified in our response to the Position Paper, there are inherent risks in any identity system and it will be critical to industry uptake that there is appropriate allocation and sharing of risk. We were pleased to see Part 3 of the Bill limits the liability of accredited entities participating in the AGDIS. However, there remain a number of gaps relating to liability that require further consideration. We have set out our recommendations below.

- ***Liability protections should extend beyond accredited entities.*** The protection afforded by section 79 only applies to limit liability of an accredited entity to another accredited entity or to a participating relying party. A lack of protection from liability to end users or the Government places a disproportionate regulatory burden on accredited entities to absorb potential loss. It is also inconsistent with the principle that accredited entities should not be liable under the AGDIS if they have complied with their obligations in good faith. We recommend section 79 of the Bill be amended so accredited entities are also protected from claims by end users or the Government.
- ***Liability caps should be introduced to limit an accredited entity's liability.*** The statutory contract regime has potential for an accredited entity to be contractually bound to many accredited entities and participating relying parties. Combined with the concerns outlined above, there is significant potential for financial exposure on an uncapped basis. We recommend the Ditigal ID Rules include provisions to cap each accredited entity's liability under each statutory contract and an aggregate cap introduced across all statutory contracts. These caps could be tied to revenue or usage and we acknowledge they should not apply where an accredited entity has acted fraudulently or criminally.
- ***The Bill should expressly exclude any liability for consequential loss.*** The lack of exclusion for consequential loss in Part 3 does not reflect market practice. We recommend the Digital ID Rules exclude consequential loss for accredited entities under the statutory contract.
- ***The protection from liability under the Bill should extend to participating relying entities.*** Although participating relying parties will not take on as many responsibilities as accredited entities, a participating relying party may breach its obligations in a way that causes loss. We recommend the same principles limiting accredited entity liability under the Bill, including those proposed above, should apply equally to participating relying entities.

2.2. The dispute resolution process should be codified in the Digital ID rules

While there is scope[1] in the Bill to make dispute resolution provisions that need to be followed before an entity can apply for an order under section 80(3), the draft Digital ID Rules contain no dispute resolution procedures. A robust dispute resolution process is critical and should be codified upfront. Combined with greater clarity around a participant's liability position as we've recommended above, we believe this will lead to greater industry uptake.We consider existing industry based external dispute resolution schemes (such as the Telecommunications Industry Ombudsman) are unlikely to be appropriate. Instead, we consider the Office of the Australian Information Commissioner (**OAIC**), which already manages privacy-related complaints, [2] may be best placed to resolve disputes relating to the AGDIS

2.3. The Bill should provide clarity on insurance requirements

Section 81 of the Bill provides scope for the Digital ID Regulator to require accredited entities to maintain adequate insurance against liability under the statutory contract regime. Given the current potential for broad, uncapped liability, it may not be possible for accredited entities to maintain adequate insurance to cover their potential liability. We recommend the Bill provide further clarity on the type, and value of, insurance cover that an accredited entity must have to be compliant. We also observe that some large corporations may elect to self-insure certain risks rather than maintain separate insurance policies, and we recommend an explanatory statement accompanying the Bill should clarify that "maintaining adequate insurance" could include self insurance of liability where that is appropriate in the context of the size and scale of the relevant organisation. We also observe cyber security insurance, particularly for large corporate entities, is difficult to obtain in the current cyber risk climate, meaning that some entities may struggle to comply with such a directive from the regulator.

03 Further clarity is needed on Reportable Incident requirements

We welcome the way the Bill separates Reportable Incidents from the Notifiable Data Breach (**NDB**) scheme, and doesn't introduce duplication of the NDB scheme. However, clarity is required on the notice thresholds and timeframes for Reportable Incidents and the definition of cyber security incidents. We propose aligning the thresholds and timeframes for reporting Reportable Incidents with existing security frameworks, in the same way the Department has done with the NDB scheme. For example, where an entity is a critical infrastructure provider, the entity would report cyber security and change control events in accordance with the Security of Critical Infrastructure Act 2018 (Cth) (**SOCI Act**) threshold and timing requirements and at the same time report them to the Digital ID Regulator.

3.1. The reporting threshold is too low

Telstra has multiple regulatory reporting requirements, and we understand the importance of ensuring the Digital ID Regulator has visibility of incidents and changes impacting the AGDIS. Where practicable, we support aligning the reporting requirements for Reportable Incidents in the Bill and Digital ID Rules with the reporting requirements under existing security regimes. This ensures consistency in the thresholds, timeframes and information being provided following an incident or change and avoids any unnecessary regulatory burden for Digital ID providers and relying parties.

The thresholds for reporting cyber security incidents in the Bill and Digital ID Rules are too low and have no regard to the impact of an incident on the AGDIS. The definition of 'cyber security incidents' also captures

1 The Bill, section 82.

attempted incidents, which may number in the hundreds a day for large entities and should be excluded from this definition. We propose that a cyber security incident should become reportable only where it impacts the availability, integrity, reliability or confidentiality of the AGDIS.

3.2. Reporting timeframes require further clarity

As the Department would appreciate, when an incident occurs, investigation is critical not only to understand the cause of the event but also to remedy and mitigate any adverse impact in a timely manner. The timeframe for reporting a cyber security incident should not begin until the reporting entity has confirmed the incident to be a cyber security incident and the relevant reporting threshold has been met.

04 Avoid duplication with existing legislation

4.1. The Bill should leverage existing legislation and avoid duplication

We recommend the Department seeks to leverage existing privacy, security and health information laws to the greatest possible extent, rather than create bespoke obligations for the security and management of information and reporting requirements under the AGDIS. For example, where an entity is a critical infrastructure provider, the reporting requirements under the Bill could be satisfied by the entity complying with the existing reporting requirements under the SOCI Act.

Several industry sectors are compelled by laws and regulations to collect identity documents from individuals prior to the provision of services (for example, for new mobile services or bank accounts). In some cases, consequential amendments to these instruments will be required to ensure the identify requirements are able to be met through the use of a Digital ID within the AGDIS.

4.2. Further clarity needed on the potential for dual penalties

The Bill prescribes civil penalties[3] for contravention of certain aspects of the legislation. However, the Bill does not state that civil penalties cannot be imposed twice for the same conduct, namely under this Bill and under another Act (for example, the Privacy Act or SOCI Act).

We recommend the Department clarify that civil penalties cannot be imposed multiple times under different legislation for the same conduct.

05 Other matters

This section of our submission contains major themes relevant to more than one aspect of the exposure draft of the legislation. In each case, we discuss our view on the possible problem we have identified and provide supporting evidence for the change in direction we recommend.

5.1. Clarify the use of existing digital identities within the AGDIS

The Bill, Digital ID Rules and the Accreditation Rules do not specify whether consumers with preexisting digital identities outside the AGDIS would be able to use their preexisting digital identities in the system in

3 Bill, Chapter 7, Part 3, Division 1, Section 119, p.104.

the event their existing Digital Identity provider becomes accredited under the AGDIS. We consider it would be a better experience for consumers if, upon accreditation of their Digital Identity provider into the AGDIS, consumers are able to use their preexisting digital identity without having to create a new digital identity.

We consider it would be helpful if either the Digital ID Rules and the Accreditation Rules clarify that upon accreditation, a consumer will be able to use their existing Digital Identity (from their Digital ID Service Provider) without having to create a new Digital Identity for the AGDIS scheme.

5.2. Harmonisation between the Identity Verification Services Bill 2023 Bill and its implementation and the Digital ID Bill, Digital ID Rules and Accreditation Rules.

Today, the various Identity Matching Services (IMSs) such as the Document Verification Service (DVS) and Face Verification Service (FVS) play a key role in many different identity verification contexts such as mobile pre-porting identity check,[4] and within the AGDIS. We note that concurrent with the development of the Digital Identity Bill, the Government is also progressing the Identity Verification Services Bill 2023.[5] To ensure consistent customer experience outcomes and reduce unintended compliance burden, regardless of whether IMS is used outside AGDIS, or as part of AGDIS, harmonisation of both Bills, and the manner in which the IMS is accessed and used inside and outside of AGDIS, is essential.

5.3. Clarify the timeframe for private sector providers and the phased approach

The four phases outlined in the guide are a pragmatic approach to gradually scaling up the AGDIS system, that as the guide notes, allows the Government to consider a range of factors before committing to further expansion. While we appreciate this approach, there are a number of additional factors we suggest warrant consideration.

Having no firm dates or anticipated duration for each phase leaves the expansion very open-ended and susceptible to a protracted rollout. There are no thresholds or guidance as to when subsequence phases can commence or whether all four phases will commence in parallel and be implemented across timelines aligned to the readiness and risk factors within each.

The private sector is keen to engage and supply services into the AGDIS, but it is not until Phase 4 that Digital IDs can be used to access “agreed Commonwealth services” and with “State, Territory and Private Services”.[6] We consider that Digital Identity has the potential to deliver substantial economic benefits to Australian businesses, both in reducing the cost of identifying customer and users of their services, and in reducing fraud. Permitting the private sector to supply Digital Identities into the AGDIS system for use in all levels of government and in the private sector (i.e., Phase 4) will further expand and realise this benefit, and we consider it would be helpful for the Department to outline an expected timeline for the four phases.

The four phases should also consider the incentives to participate, particularly for private businesses to register as a relying party. As relying parties will provide the revenue to a Digital ID Provider, low numbers or slow uptake by private businesses could be a disincentive for potential Digital Identity Providers to seek accreditation.

---

4 For example, in fulfilling mobile number pre-porting identity verification, as required under the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020. https://www.legislation.gov.au/Details/F2020L00179

5 Identity Services Verification Bill 2023. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7085

6 Your guide to the Digital ID legislation and Digital ID Rules. Same figure at the top of p.25.

In addition ensuring government is adequately funded to undertake AGDIS implementation is identified as a key factor to success. This should include education activities focussed to both citizens and businesses and adequate resourcing to enable parties to be accredited or registered in a timely manner.

It is also understood through participation in consultation activities with government, that consideration may be given to restricting specific government services to only a MyGov ID. As an alternative to this, we would suggest Government consider the option of restricting transactions which may be assessed as being 'high risk/high value' (such as engagement with specific processes in the ATO for instance) as requiring a defined higher level accreditation (obtainable by both MyGov and Private providers) or requiring a Level 3 IPV be utilised for example. This would continue to provide citizen choice across transactions, have government participate with the same conditions as the private sector and allow for the potential that into the future such transactions could be identified in the private sector also.