

10 October 2023

Department of Finance  
One Canberra Avenue  
Forrest ACT 2603

Via online form.

**Re: Digital ID Legislation and Digital ID Rules**

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission on behalf of our members and the business software industry.

**About DSPANZ**

Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world-class business software sector in Australia and Aotearoa New Zealand. Our 90+ members range from large, well-established companies to new and nimble innovators working at the cutting edge of business software and app development on both sides of the Tasman.

DSPANZ broadly supports the draft Digital ID legislation, particularly the intent to allow private sector entities to leverage myGovID.

We anticipate that many DSPs would be interested in participating in the Australian Government Digital ID System (AGDIS) as relying parties and leverage myGovID (or any other widely used, government supported credential) to simplify the sign up and sign in processes for business software.

In summary, our submission raises the following key points:

- Relationship Authorisation Manager (RAM) is critical to managing business transactions and interactions with the broader digital ecosystem. RAM must be part of AGDIS and managed independently of existing ATO systems;
- The opportunities for using Digital ID and different credentials in employee onboarding processes;
- The need for further consultation on the regulation of relying parties to make it as easy as possible for them to participate;
- The potential costs involved in participating in the AGDIS may create a barrier to entry for some DSPs acting as relying parties - especially for sign in experiences;

- Whilst the Bill intends to create a voluntary system for non-business individuals, there are going to be cybersecurity risks for individuals who choose not to have a Digital ID; and
- Digital ID is already all but mandatory for all businesses that must interact with ATO systems for GST, payroll, superannuation or business registry purposes.

We encourage the Department of Treasury (the Department) to consult further with DSPs through DSPANZ when looking at the regulation of relying parties and introducing fees in the AGDIS.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese [REDACTED] [REDACTED] for more information.

Yours faithfully,

[REDACTED]

**Matthew Prouse**  
**President & Director**  
**DSPANZ.**



### **What other types of Digital ID service should be included in the legislation, either now or in future?**

Our members have raised potential uses for Digital ID and different credentials, particularly in employee and business onboarding processes. For example, it would be useful for DSPs to check or re-verify individual attributes such as visas, working with children certificates or police checks. We support the Department looking at opportunities around verifying visas and how non-Australians could participate in the AGDIS while in Australia.

Our members have also identified potential use cases that are dependent on being able to leverage digital identity to verify the relationships and connections between individuals and the organisations and businesses they act on behalf of. Within the ABN ecosystem, it will be critical for the Relationship Authorisation Manager (RAM) to be part of the AGDIS system and be free and easy to access for digital service providers and developers of software that support natural business processes.

The potential of AGDIS may be limited if the government can only offer trusted digital identity for individuals but cannot provide verified confirmation of an individual's relationships and authorisations concerning business services. Many business processes rely upon individuals being authorised to act and transact on behalf of non-individual entities. If these interactions are dependent on existing processes and workflows that cannot leverage digital identity, then there may be limited economic benefit for business interactions.

We are also interested in ensuring that it is easy for DSPs with global teams to access myGovID, which is required to access ATO's software developer resources.

### **Are the additional privacy safeguards sufficiently robust, clear and practical?**

If DSPs are interested in becoming accredited as a Digital ID provider, they may face challenges meeting the data localisation requirement if they have global development teams.

### **What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?**

The appropriate age for young people to create and use a Digital ID should be aligned with when they can join the workforce to ensure they can access relevant government services and any software, such as payroll or time and attendance solutions, they may need for work or tertiary education.

### **What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?**

To drive the participation of private sector relying parties, the Government should make it as easy as possible for them to participate. We recommend that the ACCC or the future Regulator is a central source for security, data standards and other requirements for participating in the AGDIS.

Similar to the Australian Energy Regulator, a potential Australian Digital Regulator could centralise the technical and security accreditations, certifications, requirements and data specifications for all market participants who leverage Commonwealth Government APIs and

digital interactive services. This approach would include the security and technical requirements for access to ATO, ASIC and Fair Work Commission APIs offered today. A DSP should have a consistent set of technical, security and operational requirements - and certifications - to build software that interacts with AGDIS, CDR, ATO and ABRS services.

DSPANZ welcomes the Department undertaking further consultation on regulating private sector relying parties before it reaches this implementation phase.

While there is no intention to introduce fees for participating in the AGDIS at this stage, the legislation will allow fees to be introduced in the future. We recognise that the potential costs involved in participating in the AGDIS may be a barrier to entry for DSPs acting as relying parties. Ensuring there is widespread consultation on fees within the AGDIS will be critical for ensuring the system is ready for private sector relying parties to participate.

With the end of the Modernising Business Registers program, the Relationship Authorisation Manager (RAM) will be an invaluable resource for verifying businesses and individual's relationships to a business. For a whole of economy Digital ID system to work in Australia, it will be critical that RAM can be used across government services, is available to third parties via API and is not limited to the tax system. We support this infrastructure being managed and maintained by the same Commonwealth agency as the rest of the AGDIS infrastructure.

**What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?**

If the Department continues with a phased rollout, there may be a monopoly Digital ID provider, inhibiting any new providers from joining the AGDIS in phase 4.

**Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?**

While the Bill intends to create a voluntary system, there will be significant cybersecurity risks for individuals who do not have a Digital ID. This risk means that individuals should register with at least one Digital ID provider to protect themselves from identity theft and fraud.

Further, with the AGDIS creating a marketplace of Digital ID providers, individuals will likely need to register with every provider to protect themselves. The Department should consider options to avoid individuals needing to take these steps to protect their identity. For example, an individual could choose to only register using a single government provider - and prevent their identity documents from being used to register their digital identity on any other service. This consent model would be consistent with the 'voluntary' principle and ensure individuals had sovereignty over their identity.

We also acknowledge that it is unlikely to be a voluntary system for business participants as they are required to use Digital ID - specifically myGovID - to access ATO and ABRS services.

**Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?**

While Digital ID is voluntary and relying parties are expected to provide alternative ways to verify identity, there is still the risk that low socio-economic status individuals could be excluded from parts of the economy as the reliance on Digital ID increases.

There may also be challenges for migrants with international passports and visas who may not have the required identity documents to obtain a standard strength Digital ID, and there will need to be options for them to verify other items.