Australian Government
Department of Finance

Digital ID PIA Update 1 Departmental Responses

November 2024

Introduction

The Digital ID Act and its legislative instruments will commence on December 1, 2024. These include the Digital ID Rules, Accreditation Rules, Accreditation Data Standards, and AGDIS Standards.

A privacy impact assessment (PIA) was initially conducted in December 2023, with an addendum in January 2024, covering: the exposure draft of the Digital ID Bill and its amendments; and draft versions of the Digital ID Rules and Accreditation Rules available for public consultation in September 2023.

In July 2024, Maddocks was engaged to update the Original PIA to address proposed changes and further drafts of the Digital ID Rules, Accreditation Rules, Accreditation Data Standards, and AGDIS Standards made up to August 20, 2024. This PIA Update demonstrates the Department of Finance's dedication to a 'privacy by design' methodology for developing the Digital ID System framework.

Scope of assessment - Privacy Impact Assessment & Addendum

The PIA Update builds on the Original PIA but does not reconsider issues that were discussed, or recommendations that were made in the Original PIA. The PIA Update also does not cover changes made to the Digital ID Bill 2024, and reflected in the Act, as a result of the Bill's passage through Parliament (which occurred after the date of the Original PIA).

Like the Original PIA, this PIA Update considers the privacy impacts of the Digital ID System using the framework of the Privacy Act, including the APPs, to provide a baseline consideration of the issues, by applying the principles that sit behind each APP (which are supported by Australian and international privacy best practice).

Recommendations and departmental responses

Maddocks made the following recommendations for the Bill and Rules:

Recommendation 1	**Data localisation rules**

Rationale

Section 77 of the Act provides that the Digital ID Rules may make provision for rules to be made in relation to the holding, storing, handling or transfer of information outside of Australia. Following consultation, the intention is not to include any such rules in the Digital ID Rules on commencement in December 2024, to provide time for further consultation with industry to ensure that users of the Australian Government Digital ID System (**AGDIS**) are not precluded from using 'best-in-class security solutions that may rely on internationally hosted cloud services'.

The above approach removes the previous framework for ensuring oversight of proposed handling of information outside of Australia, and also represents a departure from the general principle in APP 8 (and similar provisions in State/Territory privacy legislation), which is intended to provide additional protections if entities intend on disclosing personal information to a recipient outside of Australia. APP 8 will apply to impose those protections only to the extent that the Privacy Act

applies to regulated entities (noting the expanded definition of personal information under the Digital ID Act), but it may not cover all data handled through the Digital ID System.

However, we acknowledge that it is important to also consider the evolution of technology which could further the general principle behind APP 8 to provide additional protections to individuals in Australia and the need to carefully consider and balance options for the Digital ID System. We also acknowledge that the Digital ID Framework will be implemented in a phased approach (by a determination to be made under s 60 of the Act). From a practical perspective, this means that on commencement of the Digital ID Rules in December 2024:

- only government entities will participate in AGDIS;
- should no rules be made under s 77 of the Act in relation to the holding, storing, handling or transfer of information outside of Australia, APP 8 will continue to apply to Commonwealth government entities in relation to any proposed transfer of personal information overseas (and any equivalent provisions under any State and Territory legislation that apply to State and Territory agencies); and
- under proposed r 3.4 of the Accreditation Rules, entities are required to map their maturity against the ISM Mapping document published by the Australian Cyber Security Centre and these controls apply irrespective of where data is held.

Recommendation

In the context of the Digital ID System being introduced in a phased approach (where other regulatory schemes will protect any personal information that is proposed to be transferred overseas on commencement), but where stakeholders have raised significant concerns about making rules requiring data localisation under the Act, we **recommend** that the Department:

- undertake to further review whether rules under s 77 of the Act are required, and commit to a timeframe for this (for example, this commitment could be made in any announcements and documentation about the phased approach);
- consider any proposed amendments to the Privacy Act prior to finalising the Digital ID Rules, to demonstrate that the final policy position taken in the Digital ID Rules in relation to data localisation takes into account any proposed privacy reforms; and
- in the Explanatory Statement to the Digital ID Rules that are made, or other guidance material on the Digital ID System, explain the security requirements that will apply irrespective of the country in which relevant data is stored, and the data localisation requirements that otherwise apply to regulated entities, to allay potential concerns about any misalignment with the principle behind APP 8.

Department's Response: Agree. The Department will further review whether rules under s 77 of the Act are required prior to phasing in private sector participation in the Australian Government Digital ID System (AGDIS), which must occur within 2 years of commencement of the Digital ID Act. In doing so the Department will consider any amendments that may have been made to the Privacy Act. The Digital ID Rules 2024 are consistent with APP 8 regarding cross-border disclosure of personal information. The Explanatory Statement to the Digital ID Rules states that APP 8 applies to all Government agencies within AGDIS, along with all existing government policies on transferring information abroad. These obligations apply irrespective of the country where the relevant personal information is stored and applies to accredited entities within AGDIS, who must also comply with strict protective security obligations under the Accreditation Rules to ensure personal information is secure and protected.

Recommendation 2 Sharing of information by the System Administrator

Rationale

Rule 4.5 of the Digital ID Rules provides that the System Administrator may share information it receives with other entities, where it considers it appropriate to do so to 'protect the security, integrity or performance' of the AGDIS. We consider the satisfaction of this specific requirement before the System Administrator can exercise its power to disclose information, to be a privacy enhancing measure. The intention of the information sharing is to enable the System Administrator, Minister, and the Digital ID Regulator, to be able to effectively perform their functions under the Act, including enforcement related functions.

However, we consider that this provision can be further strengthened by requiring the System Administrator to make a written note when it exercises its power under this provision, as a way to demonstrate the seriousness of the data sharing under this provision. This would mirror similar provisions in the Privacy Act where it is important that use of enforcement powers be properly considered and documented.

Recommendation

We **recommend** that the Department consider including in the Digital ID Rules at r 4.5, a requirement that the System Administrator make a written note if it shares information with the Minister, Digital ID Regulator or a participating entity under r 4.5, similar to the requirement at APP 6.5, where the exception in APP 6.2(e) is relied on to disclose personal information in relation to 'enforcement related activities' (as defined under the Privacy Act).

Department's Response: Agree in principle. The Department has considered this issue but does not think it necessary to include in a specific rule at this time as the System Administrator will do this practice as a matter of practice to comply with the APPs. Services Australia, when performing the pre-legislative equivalent of the System Administrator role, currently makes a note certifying that disclosures are reasonably necessary and the reason for which the disclosure is made whenever it discloses information, in accordance with APP6.2(e). The System Administrator will extend this process to cover situations where information is shared with the Minister, Digital ID Regulator or participating entity as authorised by the Digital ID legislative framework after its commencement.

Recommendation 3 Transparency about the operation of the identity exchange

Rationale

The proposed AGDIS Data Standards involve a move to a 'single blind' model for the identity exchange from the current 'double blind' model under the unlegislated Trusted Digital Identity Framework. There is a general perception that such a change will have negative privacy impacts.

However, when the other features of, and protections that have been built into, the Digital ID System are considered, the change in the technical design (to a 'single blind' model) will not increase the risk of data profiling or involve the identity exchange being able to become a central repository of identity data. It will, however, potentially involve some additional limited information about the user being able to be inferred from their choice of identity service provider. It is therefore very important that individuals are informed of the potential downstream uses and disclosures at the time they seek to obtain a digital identity with an identity service provider, including when a participating relying party will be provided details of their identity service provider.

Recommendation

We **recommend** that the Department consider mechanisms that could be employed for individuals to better understand, ideally at the time of seeking a digital identity, the potential uses and disclosures of personal information in the context of the identity exchange.

For example, the Department could seek to impose further requirements on identity service providers and/or participating relying parties, or consider working with the Digital ID Regulator and the Office of the Australian Information Commissioner to develop guidance and standard wording that could be included in relevant notices to be provided to consumers by identity service providers and participating relying parties.

Department's Response: Agree. The Department notes that some stakeholders perceive there may be privacy impacts caused by moving to a single blind. A single blind retains strong privacy protections and will continue to prevent the identity exchange from disclosing information to identity service providers on where a person uses their digital ID. Accredited services will be subject to legislative safeguards in the *Digital ID Act 2024* that prohibit data profiling. As such, the privacy impacts of moving to a single blind will likely be outweighed by the benefits the change will provide in promoting digital ID use over other identity verification methods that have greater privacy impacts and the subsequent reduced sharing and storage of personal information.

As part of the process to implement a change to a single blind model, the Department will consider how individuals could better understand the potential for their choice of identity service provider to be disclosed to a participating relying party. The Department will consider how this information should be conveyed in the context of other requirements for users to be notified and to provide consent prior to the disclosure of their personal information within the Australian Government Digital ID System.

The Office of the Australian Information Commissioner (OAIC) will work with the Department to help individuals understand the privacy protections in the Digital ID system, including the operation of the 'single blind'.