Australian Government
Department of Finance

Attachment A
Digital ID PIA Departmental Responses

18 January 2024

Introduction

In November 2023, Maddocks undertook a privacy impact assessment (PIA) for the Department of Finance (Finance) on the exposure draft of the Digital ID Bill published by Finance on 19 September 2023 (Exposure Bill) and consultation drafts of the Digital ID Rules 2024 and the Digital ID Accreditation Rules 2024 (together referred to as the Rules).

The Digital ID Bill 2023 was introduced in the Senate on 30 November 2023 and referred to the Senate Economics Legislation Committee. The text of the Digital ID Bill 2023 differs in some respects to what was in the Exposure Bill.

Finance is committed to ensuring that any privacy impacts that may flow from the changed text reflected in the Digital ID Bill 2023 is appropriately considered. Finance commissioned an addendum to the PIA (Addendum) undertaken by Maddocks, which assessed these changed portions of text.

The recommendations in this document and the associated departmental responses are the result of both the PIA and Addendum assessments.

Scope of assessment - Privacy Impact Assessment & Addendum

Finance, as the Australian Government agency with key responsibility for the Bill, commissioned Maddocks to undertake a PIA. The PIA considered whether the privacy impacts of the proposed legislative scheme have been identified and appropriately managed or minimised in the accreditation scheme and Australian Government Digital ID System (AGDIS).

PIAs in respect of proposed new legislation require a slightly different approach to other PIAs that consider the handling of personal information in projects under an existing legislative regime, which involve an analysis of that handling against the APPs in the Privacy Act. The Privacy Act expressly permits the handling of personal information which is ‘required or authorised’ by an Australian law. For PIAs such as this one, which require consideration of a proposed new Australian law, the question is whether the proposed Australian law should provide that authorisation.

The PIA and Addendum considered 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. These 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 Clarifying meaning of 'personal information'

Rationale

The Bill provides a standalone definition of 'personal information' at cl 9 which in substance replicates the current definition of 'personal information' in the Privacy Act, and extends the definition to include 'attributes' (as defined) of individuals. However, given the language in cl 33 of the Bill (which extends the operation of the definition of personal information in the Privacy Act), there may be some uncertainty about whether the definition of 'personal information' is intended to be fixed as at the enactment of the Bill.

The Australian Government released its response to the Privacy Act Review Report in September 2023 which included an in principle agreement to adopt a more expansive concept of 'personal information' in the Privacy Act, to effectively include some technical and inferred data (e.g., IP addresses and other device identifiers).

There is a risk that the Privacy Act and the Bill may become misaligned in respect of information that will be 'personal information' under the Privacy Act in future, but not otherwise picked up in the meaning of 'attribute' in the Bill.

Recommendation

We **recommend** that the Department consider refining the drafting of the Bill to:

- define personal information in cl 9 of the Bill to simply reference the definition in the Privacy Act (which may change over time), so that cl 33 will then operate to include 'attributes' to the extent not already covered by any expanded definition; or
- make it clear whether the intention is to have a fixed definition of personal information as it is currently in the Privacy Act (but as extended to include attributes).

In either case, we suggest that the Explanatory Memorandum to the Bill clearly explain whether the intention is for the definition of personal information to change as the definition in the Privacy Act is updated following any Privacy Act reforms or not, and why that policy position has been taken.

Department's response: Agreed in part. The Department has considered this issue and is of the view that it is impractical to retain both a moving element of the definition (i.e., that changes when the Privacy Act changes) and a fixed element, as the definition may be inconsistent if the moving element changes. The intention of the current approach is that if the definition of 'personal information' in the Privacy Act is amended, consequential legislation would be introduced to ensure that the Bill (as enacted) remains consistent with any amended definition and additional requirements in the Privacy Act. The Department has made this clear in the Explanatory Memorandum.

Recommendation 2	Matters to be taken into account for accreditation – other privacy breaches

Rationale

Safeguarding the personal information of individuals is key to ensuring that there is social licence for the Digital ID Scheme. In this context, if an entity breaches the privacy of an individual in respect of any of its other services and functions (whether under the Privacy Act or other legislation), this should be able to be taken into account by the Digital ID Regulator when considering whether or not to accredit that entity for the provision of Digital ID services, and also in decisions about whether or not that accreditation should be maintained.

The Digital ID Rules already provides for this to be taken into account in relation to entities that have been subject to certain Information Commissioner determinations under the Privacy Act or similar determinations under a similar law of a foreign jurisdiction (see Rule 5(1)(c) of the Digital ID Rules). However, this would not extend to any finding or determination of a State or Territory privacy regulator. We consider that ensuring that this can be taken into account as part of the accreditation process would provide further assurance to the Australian public that all entities participating in the Digital ID Scheme are considered 'safe' to handle personal information in the context of the accredited service.

Recommendation

We **recommend** that the Department consider expanding Rule 5(1)(c) of the Digital ID Rules so that the Digital ID Regulator may also have regard to findings and determinations of a similar nature of a State or Territory privacy regulator.

Department's response: Agreed-in-principle. The Department considers that the Digital ID Regulator should be able to take all relevant matters into account. The Department will consider whether this is already covered by Rule 5(1)(b) and consider other feedback on the Rules. If a rule change is appropriate the Department will make a recommendation to the Minister.

Recommendation 3 Guidance on concepts included in the Bill

Rationale

In addition to the Information Commissioner's functions under the Privacy Act, clause 40 of the Bill sets out that an additional function of the Information Commissioner is to provide advice on request of the Digital ID Regulator on matters relating to the operation of the Bill. Section 28 of the Privacy Act provides for the Information Commissioner's guidance related functions under the Privacy Act. All the powers conferred on the Information Commissioner under the Privacy Act equally apply to the Digital ID Scheme.

Stakeholders have raised a number of concerns during the consultation period about the meaning of certain concepts in the Bill, and we agree that ensuring that accredited entities can understand their obligations under the legislative framework will be key to ensure that the privacy protections are implemented in practice. This is particularly the case for some privacy protections in the Bill, such as ensuring that consent is obtained, which might be implemented by accredited entities anywhere along a compliance spectrum (from minimum requirements only, to full privacy best practice), particularly where the Bill does not define these terms, or import relevant concepts under the Privacy Act.

We see benefit in the Information Commissioner issuing guidance on privacy matters related to the Digital ID Scheme, particularly if language in the Bill and Rules is not further clarified. For example, guidance could be provided on the requirements for valid 'consent' in the various contexts of the Digital ID Scheme, the proper interpretation of 'collect', 'disclose' and 'hold' in the Bill and Rules, the meaning of 'intentional' collection, and what steps an accredited entity should take before disclosing personal information to a relying party.

We believe such guidance would be particularly helpful by ensuring compliance with privacy best practice during the period before introduction of proposed reforms to the Privacy Act. We think this would benefit individuals using their digital ID under the Digital ID Scheme, and minimise the adverse effects on the privacy of individuals.

Recommendation

We **recommend** that the Department work with the Information Commissioner to consider the stakeholder feedback provided during the consultation period, particularly on the meaning of different concepts in the Bill which stakeholders considered could benefit from being further defined or having guidance provided, to inform the Information Commissioner's approach to preparing any specific guidance in relation to the Digital ID Scheme**.**

Department's response: Agreed. The Department will assist the Information Commissioner to develop any guidance material they decide to prepare.

Recommendation 4 Arrangements between the co-regulators

Rationale

We expect the Digital ID Regulator and Information Commissioner will work cooperatively in administering the Digital ID Scheme. However, it will be important to ensure that individuals who are aggrieved have a seamless experience in having their complaints addressed.

Recommendation

We **recommend** that consideration be given to whether additional measures are required to facilitate the co-regulated nature of the Digital ID Scheme. For example:

- providing in the Bill that the Digital ID Regulator and the Information Commissioner will develop a Charter setting out the commitments of the Digital ID Regulator and the Information Commissioner in undertaking their respective regulatory functions, including flows of information where one receives a complaint that is more appropriately handled by the other; or
- the Department work with the Digital ID Regulator (once established) and the Information Commissioner to ensure there are appropriate administrative arrangements in place about how the co-regulators will work together and ensure there is publicly available information about this.

Department's response: Agreed. The Bill includes provisions for information-sharing between regulators. The Department does not believe that further refinement of the Bill is required, but will work with the ACCC and the Information Commissioner to ensure that the co-regulators work effectively together to ensure individuals seeking to make a complaint have a seamless experience in having their complaint addressed.

Recommendation 5	Accredited entities reporting on PIA implementation

Rationale

The Accreditation Rules require accredited entities to undertake PIAs in certain circumstances and provide their responses to any recommendations (and we see these as important privacy protections). However, there does not appear to be a mechanism to monitor whether an accredited entity has in fact undertaken any steps that it has indicated that it will do in response to a PIA recommendation. This may undermine the otherwise robust process.

Recommendation

We **recommend** that the Accreditation Rules provide that an accredited entity is required to report on the implementation of any actions it has indicated it will undertake in a response to a recommendation in a PIA (for example, as part of the annual review process).

Department's response: Agreed-in-principle. The Department agrees accredited entities should be required to report on their implementation of PIA recommendations. Any proposed changes to Rules 6.2(6) and (7) in the draft Accreditation Rules to address this recommendation, will be provided to the Minister for their decision.

Recommendation 6	Requirements for express consent

Rationale

In various different contexts, the Bill and Rules require that the 'express consent' of the individual is required to authorise the handling of personal information, however this wording is not currently included in some provisions, which may imply that implied consent is sufficient. We understand that this is not consistent with the policy intent.

Recommendation

We recommend that the drafting of the Bill and Rules be reviewed to ensure that all instances where consent of an individual is required refer to a requirement for 'express consent' (see for example clauses 46(3)(b), 47(2)(b) and 47(5)(c)(ii)).

Department's response: Agreed. The Department agrees and has already made these amendments to the Bill. The version of the Bill currently before Parliament, ensures that all instances where consent of an individual is required refers to a requirement for 'express consent'.