Maddocks

Department of Finance

Privacy Impact Assessment Addendum

Digital ID Bill and Rules

Date of analysis – 1 December 2023

Date of finalisation – 9 January 2024

Contents

1. Introduction

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

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

1.3 The Department wishes to ensure that any privacy impacts that may flow from the changed text reflected in the Digital ID Bill is appropriately considered, and accordingly has commissioned this addendum to the PIA (**Addendum**).

1.4 This Addendum is intended to inform the Department, the Australian Parliament, and stakeholders about any additional privacy impacts in the Digital ID Bill. Like the approach taken in the PIA, we have used the APPs contained in the *Privacy Act 1988* (Privacy Act) as a framework to consider, from a principles basis, any privacy impacts.

1.5 The Addendum only covers those matters that were not included in the Exposure Bill, or which have substantially changed since the Exposure Bill. This Addendum should be read with the PIA, including the terms set out in the Glossary in **Part D** of the PIA, as well as the text of the Digital ID Bill.

2. Short Description of Changes Between the Exposure Bill and the Digital ID Bill

2.1 In summary, the Digital ID Bill:

2.1.1 includes a new civil penalty offence for any entity that holds itself out as an accredited entity where this is not the case (Digital ID Bill, cl 31);

2.1.2 clarifies the entities that can enter into an APP-equivalent agreement (Digital ID Bill, cl 34; Exposure Bill, cl 32);

2.1.3 makes clear the circumstances in which the Information Commissioner may share information (Digital ID Bill, cl 43);

2.1.4 clarifies the wording in relation to when an accredited entity can collect prohibited attributes (Digital ID Bill, cl 44; Exposure Bill, cl 41);

2.1.5 expressly specifies that accredited entities can disclose unique identifiers of an individual to their contractors (Digital ID Bill, cl 47; Exposure Bill, cl 44);

2.1.6 clarifies when accredited entities may collect, use and disclose biometric information, including circumstances when biometric information can be disclosed to law enforcement agencies (Digital ID Bill, cl 49; Exposure Bill, cl 46);

2.1.7 clarifies the functions of the Digital ID Regulator (Digital ID Bill, cl 91; Exposure Bill, cl 86);

2.1.8 includes a new role of a System Administrator (Digital ID Bill, Chapter 6); and

2.1.9 clarifies interactions with tax file number offences (Digital ID Bill, cl 161).

3. Discussion of Potential Additional Privacy Impacts

Prohibition on holding out as an accredited entity

3.1 The Digital ID Bill now includes cl 31 which provides that an entity must not hold out that it is an accredited entity if that is not the case. This is a civil penalty provision, enforceable by the Digital ID Regulator under Part 6 of the Regulatory Powers Act.

3.2 We consider that the inclusion of this prohibition furthers the principle behind APP 1. The provision promotes transparency about participants who are subject to the privacy protections in the Digital ID Bill, including the participants in the AGDIS, by acting as a deterrent to non-accredited entities from acting in a manner that may cause the public to believe that those protections apply.

APP-equivalent agreements

3.3 New sub-clause 34(2) clarifies that the Minister may on behalf of the Commonwealth enter into an APP-equivalent agreement with a department or authority of a State or Territory.

3.4 This wording clarification furthers the intention that, if a department or authority of a State or Territory is not subject to the Privacy Act[1] nor State/Territory privacy laws, the Minister can enter into an APP-equivalent agreement where the entity agrees to abide by the APPs. This means that another type of non-APP entity (such as a small business operator) cannot enter into an APP-equivalent agreement, and therefore cannot rely on such an agreement to satisfy the requirement for handling personal information in cl 36 (which can be summarised as meaning that an accredited entity must not do an act or engage in a practice with respect to personal information unless the Privacy Act applies; or a comparable State or Territory privacy law applies; or the entity has an APP-equivalent agreement with a requirement to comply with the APPs in it).

3.5 This effectively means that, should another type of non-APP entity such as a small business operator achieve accreditation, it would not be able to handle personal information unless the Privacy Act applies to that entity (for example, because it has opted in to being treated as an organisation under section 6E of the Privacy Act).

3.6 We consider this to be a privacy positive measure, including by ensuring that accredited entities that may not otherwise be covered by privacy laws are subject to privacy oversight.

Sharing of information by the Information Commissioner

3.7 Under the Privacy Act, the Information Commissioner may share information with other authorities (for example, an enforcement body or a State privacy regulator (Privacy Act, s 33A)) or disclose information in the public interest (Privacy Act, s 33 B). New cl 43 of the Digital ID Bill makes clear this also applies to the Information Commissioner where they are undertaking privacy related functions under the Digital ID Bill.

3.8 We consider that this measure, to put beyond doubt the powers of the Information Commissioner in connection with their co-regulatory role, is a privacy enhancing measure as it will enable the Information Commissioner to undertake their role more effectively, including referring matters to other relevant authorities.

3.9 We expect the Information Commissioner to be acutely aware of the importance of ensuring that only the minimum amount of personal information necessary is disclosed when undertaking their role, and of considering not only whether personal information *can* be disclosed but also whether it *should.*

[1] State or Territory authorities are not usually bound by the Privacy Act (although can request to be prescribed so that they are treated as an 'organisation' for the purposes of the Privacy Act under section 6F of the Privacy Act).

Collection of prohibited attributes by accredited entities

3.10 The Exposure Bill prohibited the 'intentional' collection of certain attributes of individuals (Exposure Bill, cl 41), including information which most people would consider particularly sensitive (such as an opinion about an individual's racial or ethnic origin, religious beliefs or sexual orientation or preferences). As set out in the PIA, the use of the word 'intention' in the context raised a particular risk that, without further clarification, accredited entities would take different approaches in applying the law.

3.11 The Digital ID Bill now no longer requires that there be an 'intentional' collection of prohibited attributes - rather it provides a general bar to collection with exceptions (Digital ID Bill, cl 44). We consider the exception at cl 44(2) to be reasonable, noting that it requires accredited entities to destroy any prohibited attributes it has collected (which it had not solicited). New cl 44(3) also clarifies that attributes may be collected even if prohibited attributes can be reasonably inferred from the collection. The Digital ID Bill provides an example of this is where an individual's racial or ethnic origin can be reasonably inferred from the individual's name or place of birth. However, the entity can nevertheless collect the individual's name and place of birth. We consider this approach in cl 44(3) to be pragmatic.

3.12 We consider the clarification to the wording in cl 44 to be a privacy positive measure as it provides greater clarity for when entities can collect personal information and furthers the data minimisation principle that is a part of APP 3.

Disclosure of unique identifiers to contractors

3.13 Clause 44 of the Exposure Bill set out when an accredited entity can disclose a unique identifier that it has assigned to an individual. This has been updated in cl 47 of the Digital ID Bill which now specifically provides that an accredited entity can disclose the unique identifier to a contractor of the accredited entity for the purposes of the contractor providing an accredited service of the accredited entity.

3.14 We consider the change is consistent with the principle in APP 9, which acknowledges that in certain circumstances unique identifiers (that are government identifiers) may need to be used by contracted service providers to discharge their contractual obligations to an agency or a State or Territory authority (APP 9.2(b)). Clause 47 of the Digital ID Bill extends this principle further (so that use and disclosure of a government related identifier will be authorised under APP 9.2(c) because of the application of an Australian law, even if the accredited entity is not an agency or State/Territory authority). However, we observe that the appropriateness of the involvement of an accredited entity's contractors in providing an accredited service will be considered as part of the accredited entity obtaining, and maintaining, its accreditation (including that the contractor's systems and processes for handling personal information will be considered as part of a privacy impact assessment and security assessment processes – see the discussion in the PIA).

3.15 Accordingly, we consider that the privacy risks associated with the change to this provision have been appropriately mitigated.

Collection, use and disclosure of biometric information

3.16 As discussed in the PIA, the collection, use and disclosure of biometric information is one of the key issues for stakeholders for the Digital ID Bill. The language in cl 49 of the Digital ID Bill (previously cl 46 of the Exposure Bill) has now been clarified. The most substantive change is to cl 49(3), which now provides that an accredited entity is authorised to disclose biometric information of an individual to a law enforcement agency (within the meaning of the *Australian Crime Commission Act 2002*) only if:

3.16.1 the 'disclosure of the information is required or authorised by or under a warrant issued under a law of the Commonwealth, a State or a Territory'; or

3.16.2 with the 'express consent' of the individual concerned for an investigation/prosecution or identity verification.

3.17 Under the Exposure Bill, the disclosure to a law enforcement agency under a warrant required the warrant to be issued by a 'magistrate, judge or tribunal member' (Exposure Bill, cl 46(3)). A 'law enforcement agency' is the Australian Federal Police, police force of a State of a Territory, or any authority or person responsible for the enforcement of the laws of the Commonwealth, State or Territory. The third limb of the definition of 'law enforcement agency' has the potential to include a wide range of entities.

3.18 We note that while warrants are usually issued by judicial officers and tribunal members, there may be circumstances where a particular warrant may be able to be issued by other persons as provided for under a relevant law. This may be of concern to some who expect, given the seriousness of warrants because of the potential impact on an individual's affairs, that warrants should be limited to being issued by judicial officers and tribunal members.

3.19 However, in our view the revised wording maintains the objective scrutiny from a body other than the law enforcement agency seeking to obtain the biometric information (which we noted was a key feature discussed in the PIA). We consider where the relevant parliament has considered it appropriate that a person, other than a judicial officer or tribunal member, may issue a warrant (with the underlying assumption that any such person would undertake their duties with integrity) then we consider that the change in wording in the Digital ID Bill does not raise any additional privacy impacts.

3.20 We consider the requirement for the warrant to require or authorise the disclosure of the biometric information to be a relatively high bar. However, we note that there may be concerns by some that warrants could potentially be issued in respect of matters which objectively do not require biometric information. In our view, this is an issue broader than the Digital ID Bill. It goes to the integrity of the law enforcement agency seeking a warrant (and being able to justify the need for particular information) and that of the person authorised to issue the warrant, who must objectively consider the information presented to them in deciding whether to issue the warrant. Should these entities fail to discharge their public duties with integrity, the appropriate forum to address this is through other oversight bodies and mechanisms. From a privacy perspective, the accredited entity will need to ensure it has in place processes to review any warrants it may receive to check they do in fact require or authorise the relevant biometric information sought.

3.21 We also consider the clarification that the consent of an individual must be 'express' before it can be relied upon by an accredited entity to disclose the individual's biometric information, to be a privacy enhancing measure. This will ensure that individuals have greater control over how their biometric information is handled by effectively requiring recording of the specific permission that individuals' provide.

Functions of the Digital ID Regulator

3.22 The Digital ID Bill now specifically sets out at cl 91 a comprehensive list of functions of the Digital ID Regulator. This change to the wording does not raise any further privacy impacts.

3.23 Sub-clause 91(f) specifically provides that the Digital ID Regulator has a function to share information with the Minister, System Administrator, the Digital ID Data Standards Chair and the Information Commissioner. We consider, to the extent that this information may include personal information, it is appropriate to be shared with the relevant entities administering the scheme or a role under the scheme. The Digital ID Regulator will need to be confident when proposing to disclose any personal information that the receiving entity has a need-to-know that personal information. However, we consider this to be a business process issue to be settled as part of establishing the Digital ID Regulator

Functions of the System Administrator

3.24 The Digital ID Bill now includes a Chapter 6 on the System Administrator for the AGDIS, the Chief Executive Centrelink. The System Administrator has the responsibility for managing the availability of the AGDIS and identifying and managing operational risks.

3.25 We do not consider the role of a System Administrator introduces any further privacy risks or impacts. We note that a key to ensuring the well functioning of the AGDIS is for the System Administrator to work effectively with the other oversight bodies (the Minister, the Digital ID Regulator, the Digital ID Data Standards Chair and the Information Commissioner), including sharing relevant information (cl 95(i)). Like the Digital ID Regulator, the System Administrator will also need to be confident when proposing to disclose any personal information that the receiving entity has a need-to-know that personal information. However, again we consider this to be a business process issue.

3.26 As discussed in Recommendation 4 in the PIA, with the introduction of another body involved in the administration and regulation of the AGDIS, it will be important to ensure that individuals who are aggrieved have a seamless experience in having any complaints addressed. We expect that the Department's proposed implementation of Recommendation 4 could be extended to ensure that appropriate arrangements are in place to ensure that the Digital ID Regulator, the Information Commissioner and the System Administrator work effectively together.

Interaction with tax file number offences

3.27 The Digital ID Bill now clarifies that nothing in the Bill affects or limits the operation of certain other laws. Sections 8WA and 8WB of the *Taxation Administration Act 1953* contain offences for unauthorised use etc. of tax file numbers. Section 17 of the Privacy Act requires the Information Commissioner to issue rules concerning the collection, storage, use and security of tax file numbers.

3.28 We consider this clarification recognises the sensitive nature of tax file numbers and the addition protection provided under the Privacy Act.