Office of the Victorian Information Commissioner

[redacted]

11 October 2023

[redacted]

Online submission

Submission in response to the 2023 draft Digital ID legislation

Thank you for the opportunity to comment on the 2023 draft Digital ID Legislation comprised of the exposure draft Digital ID Bill (**Bill**) and the draft Digital ID Rules (**Rules**).

The Office of the Victorian Information Commissioner (**OVIC**) has combined oversight of freedom of information, information privacy and information security, administering both the *Freedom of Information Act 1982* (Vic) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**). As such, my office has a particular interest in Australia's digital ID system and its impact on the privacy and security of the public's information.

OVIC understands the Bill seeks to establish the foundation for Australia's digital ID system by, among other things:

- Legislating a voluntary accreditation scheme for Digital ID providers in the public and private sector to promote trust in digital ID services across the economy.
- Providing a legislative basis for expanding the existing Australian Government Digital ID system (**AGDIS**). This will enable the AGDIS to include Digital IDs provided by states and territories, and eventually, private sector providers that are approved to participate in the system. As a result, the public will have more choice over which digital ID provider to use to access services, both at federal and state level. In time, the public will be able to use a private sector digital ID to access government services participating in the AGDIS.
- Establishing a Digital ID Regulator (**the Regulator**).

This submission responds to a number of questions in the *Guide to the Digital ID legislation and Digital ID Rules* (**the Guide**) and comments on some matters relevant to draft provisions in the Bill and the Rules. For ease of reference, this submission adopts the definitions used in the Bill.

The following section responds to questions in the Guide.

Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions be improved?

1. OVIC understands that, initially, three types of digital ID services will be accreditable: identity service providers, identity exchange service providers and attribute service providers. The Bill allows for other types of services to be prescribed to accommodate the evolving digital ID landscape.

2. Accreditation is subject to conditions specified in the Act, the Accreditation Rules, and imposed by the Regulator.[1] Section 18(2) of the Bill gives the Regulator discretion to impose conditions on the accreditation of an entity either at the time of accreditation or at a later time, if the Regulator considers it appropriate in the circumstances. Conditions may also be imposed on request by the entity.[2] Conditions may relate to a range of matters including:

    - any limitations, exclusions, or restrictions on the accredited services of the entity;[3]
    - the kinds of restricted attribute[4] and biometric information the entity is authorised to collect, use or disclose and the circumstances in which it may be collected, used or disclosed;[5]
    - the entity's information technology systems through which the entity's accredited service are provided;[6] and
    - actions that the entity must take before its accreditation is suspended or revoked.[7]

3. OVIC suggests amending section 18 to include a non-exhaustive list of factors the Regulator should have regard to when considering whether to impose conditions on an entity's accreditation and the nature of those conditions. The factors could include:

    - the risk assessments the entity has conducted such as privacy impact assessment and security risk assessment;
    - the entity's data breach management plan;

[1] Bill, section 17.
[2] Bill, section 18(3).
[3] Bill, section 18(5)(a).
[4] Bill, section 11, meaning of restricted attribute.
[5] Bill, sections 18(5)(c) and (d).
[6] Bill, section 18(5)(e).
[7] Bill, section 18(5)(f).

4. Specifying factors the Regulator should consider, including factors that are privacy and security focussed, will support the Regulator to not only determine the conditions, if any, that are necessary but also whether the accredited entity will be able to comply with those conditions.

5. For example, section 19 outlines requirements the Minister must comply with before making Accreditation Rules relating to restricted attributes or biometric information. Before the Minister can make Accreditation Rules that authorise the collection, use or disclosure of restricted attributes or biometric information, the Minister must consult with the Information Commissioner and must have regard to five factors. These factors include potential harm resulting from disclosure of the information, community expectations, whether disclosure is regulated by another Commonwealth law, any privacy impact assessment that has been conducted, and any other matter the Minister considers relevant.

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

6. OVIC notes a range of privacy and security protections entrenched in the Bill, including the additional privacy safeguards which apply to all accredited entities regardless of whether they participate in the AGDIS.[8] The comments below touch on OVIC's view on some of the privacy safeguards in the Bill.

Express consent required for handling of specific attributes and biometric information

7. There are a number of provisions in the Bill which require accredited entities to obtain express consent from an individual before collecting, using or disclosing their information. For example:

    - Section 42 prohibits an accredited entity from disclosing specific attributes of an individual to a relying party[9] without the express consent of the individual.[10]

    - Section 43 prohibits an accredited entity from disclosing a restricted attribute to a relying party without express consent of the individual.

    - Section 45 allows an entity to collect, use and disclose biometric information only with the express consent of the individual to whom the information relates, with some exceptions.

8. While consent is an important mechanism for giving individuals control over how their information is handled, and it is one of the key principles underpinning the digital ID system, the consent will only be effective if it is valid.

[8] Bill, sections 41-53.
[9] Bill, section 9, definition of relying party.
[10] The attributes include the individual's name, address, date of birth, phone number, email address and any attribute prescribed by the Accreditation Rules.

9. There are five elements that must be satisfied for consent to be valid. It must be voluntary, informed, specific, current, and the individual must have capacity to consent. OVIC recommends the Bill include a definition of consent that specifies these five elements of consent. This will ensure entities turn their minds to each of the elements when seeking to rely on consent to handle information.

Prohibition on data profiling

10. Section 50(1) and 50(2) prohibit accredited entities from using or disclosing personal information for data profiling even if the individual has consented to that use or disclosure. However, section 50(3) creates exceptions to the prohibition including where the information is used for purposes relating to the entity providing its services (such as improving the performance or useability of the entity's information technology systems).

11. OVIC is concerned that permitting certain types of profiling is likely to increase the risk of scope creep or further types of profiling being authorised in future. This would not only increase privacy and security risks for individuals but would also impact the public's trust and confidence in the digital ID system. While OVIC understands the need for service providers to improve their software, they should use dummy or synthetic data for such purposes rather than the personal data of individuals.

Restriction on using or disclosing personal information for enforcement purposes

12. Section 51 permits an accredited entity to use or disclose personal information to an enforcement body conducting enforcement related activities even where those activities do not relate to the AGDIS or the handling or misuse of a digital identity.

13. In OVIC's view, an enforcement body should only be able to access personal information for offences related to the AGDIS. Further, any use or disclosure of personal information under warrant should be for offences related to the digital ID system. For instance, OVIC considers section 51(1)(d) appropriate as it allows accredited entities to use or disclose personal information to an enforcement body for the purposes of reporting digital ID fraud incidents or cyber security incidents.

14. Given the wide range of personal information collected, used and disclosed for purposes of the Bill, permitting a law enforcement body to access the information for a broad range of offences carries the real risk of enabling the law enforcement body to conduct unnecessary and intrusive surveillance on individuals. Such surveillance is unlikely to align with community expectations of how their personal information should be handled under this Bill. Further, it would undermine the community's trust in the digital ID system. Access by law enforcement should therefore be strictly limited, and where it does occur, statutory oversight is recommended.

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

15. OVIC understands the expansion of the AGDIS to states and territories and the private sector will occur in four phases:[11]

    - Phase 1 – adding more services to the AGDIS including state and territory services
    - Phase 2 – enabling access to Commonwealth services using a digital ID issued by accredited identity providers in other jurisdictions
    - Phase 3 – enabling customers to use their digital ID issued by either Commonwealth or state and territory identity providers to access private sector services
    - Phase 4 – allowing customers to access some government services using digital IDs issued by accredited private sector digital ID providers

16. The Bill authorises the Minister to determine who can apply to the Regulator to participate in the AGDIS.[12] The phased approach is intended to allow the Government to consider various factors before committing to further expansion including the maturity of the digital ID market, penetration of the accreditation scheme, and the capacity of the relevant agencies such as Services Australia (as the accredited identity exchange provider in the AGDIS).[13]

17. In OVIC's view it would also be important for the responsible Minister to consider the annual reports of the Regulator and the Information Commissioner which would set out a range of matters relevant to the operation of the AGDIS including[14]:

    - The number of applications received for accreditation or approval to the AGDIS
    - The number of reportable incidents that have occurred in the AGDIS
    - The number of accreditation suspensions or revocations
    - In relation to the Information Commissioner's report, information about the Information Commissioner's functions and exercise of their powers with respect to the privacy aspects of the Bill.

18. OVIC also recommends the Minister consult with the Regulator and the Information Commissioner including any other relevant agencies, to assess whether the digital ID system is operating effectively and efficiently before expanding to another phase.

[11] Guide, page 25.
[12] Bill, section 57.
[13] Guide, page 25.
[14] Bill, section 144 and 145.

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

19. Section 71 of the Bill prohibits a relying party participating in the AGDIS from requiring an individual to create or use a digital ID to access the service of the relying party. The relying party must provide an alternative way for an individual to verify their ID, such as by phone, in person or online. OVIC also suggests that alternative verification methods should be developed in conjunction with accessibility in mind, and that consultation with community groups representing people from diverse backgrounds or with disabilities should be considered.

20. OVIC supports the requirement for voluntary use of a digital ID as it minimises the barriers to accessing Commonwealth government services.

21. However, OVIC notes section 71(3) provides exceptions to the voluntary requirement including where the "law of a Commonwealth, State or Territory requires verification of an individual's identity solely by means of a digital ID".[15] If use of digital ID is intended to be voluntary, OVIC queries why the Bill would permit government services to require an individual to use a digital ID to access those services.

22. Further, section 71(4) allows the Regulator to grant an exemption from the voluntary requirement to a participating relying party that is a small business or provides its services solely online.[16] OVIC is concerned that enabling the Regulator to grant exemptions to small businesses and/or online businesses will have a negative impact on an individual's right to choose whether to create and use a digital ID. Particularly if the Regulator grants exemptions to a large number of businesses.

23. While there may be circumstances in which it is appropriate for the Regulator to grant an exemption, it will be crucial for the Regulator to exercise this power prudently. OVIC notes that the Regulator is prohibited from granting an exemption to Commonwealth government services. As the AGDIS expands to include State and Territory government agencies, it will be crucial to ensure the use of digital ID remains voluntary.

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

Data localisation requirement

24. OVIC notes the prohibition in section 73 of the Bill and Rule 10 on accredited entities holding, storing, handling or transferring information that is or was generated, collected, held or stored in the AGDIS outside Australia, with some exceptions.

[15] Bill, section 71(3)(a).
[16] Bill, sections 71(5)(a)and 71(5)(b).

25. Given the range of personal information involved in the digital ID system, data localisation minimises the risk to privacy by ensuring the information is subject to protections in the Bill. In addition, the prohibition helps improve the security of individual's information by ensuring information such as sensitive information and biometric information remains within Australia. Further, section 73 is likely to align with community expectations of how their information is handled within the AGDIS.

26. OVIC notes that the Minister may grant an accredited entity an exemption to the data localisation requirement.[17] OVIC notes the Minister is required to consider specific matters when deciding whether to grant any exemption, including the entity's risk assessment plan, privacy impact assessment, and the effectiveness of the entity's protective security arrangements.[18]

Comments on draft provisions in the Digital ID Bill

Deactivation and de-identification of digital ID and personal information

27. Section 28 requires an accredited identity service provider to deactivate an individual's digital ID on request as soon as practicable after receiving the request.

28. OVIC suggests the Bill be amended to include a requirement for the accredited entity to delete the individual's digital ID on request as soon as practicable. There should also be a requirement for the entity to inform the individual of the option to delete their digital ID so the individual is aware of their options. Given the creation of a digital ID is intended to be voluntary, OVIC considers it appropriate to provide a mechanism for individuals to delete their digital ID should they no longer wish to have one.

29. In relation to the AGDIS, section 130 requires accredited entities that hold an approval to participate in the AGDIS to destroy or de-identify personal information in their possession or control if no longer required or authorised to retain it. This requirement also applies to accredited entities whose approval is suspended or revoked.

30. All de-identified information carries the inherent risks of re-identification. Further, it is often challenging to comprehensively assess the risk of re-identification, and therefore implement measures to manage that risk, as it would require knowledge of all auxiliary information available that may be combined with the de-identified information. OVIC recommends section 130 be amended to remove the reference to de-identification, and instead require accredited entities to destroy personal information once the entity is no longer required or authorised to retain it.

[17] Rule 10(5).
[18] Rule 10(7)(a).

Regulation of the digital ID ecosystem

31. OVIC understands the digital ID ecosystem will be regulated by several bodies:

    - The Australian Competition and Consumer Commission (**ACCC**) will be the inaugural Regulator[19] responsible for governing the accreditation scheme, approving entities to participate in the AGDIS and enforcing compliance with the non-privacy aspects of the legislation, among other things;

    - The Office of the Australian Information Commissioner OAIC will have oversight over the privacy aspects of the legislation, both in relation to the accreditation scheme and the AGDIS; and

    - Services Australia will administer the AGDIS and be responsible for operational aspects of the AGDIS including identifying and managing risks, managing digital ID fraud incidents and cyber security incidents, and other matters related to the integrity and performance of the AGDIS. OVIC notes the sharing of functions between Services Australia and the ACCC remains under consideration.[20]

32. These oversight bodies must be sufficiently resourced to undertake their functions under the Bill. For instance, the ACCC will require appropriate funding and resourcing to ensure it can effectively audit accredited entities and monitor compliance with the Bill, to ensure the public's information is being handled appropriately. Similarly, the OAIC will need to be adequately funded and resourced to undertake its new functions under the Bill.

33. OVIC suggests that relying on Services Australia to audit a system that is crucial to the operation of Service Australia's online services poses an impossible conflict of interest. OVIC suggests an alternative, independent security auditor be given this role. For the auditor to be truly independent it should have no other business with either Services Australia or other entities in the AGDIS. Ideally, the scope of the Digital ID Regulator should be expanded to provide oversight of information security throughout the Digital ID ecosystem, and additional resources provided for this purpose.

Annual report by Digital ID Regulator

34. The Regulator will be required to provide an annual report to the Minister. Section 144(2) sets out the information that must be included in the report. To increase transparency in the digital ID system, OVIC recommends the provision be amended to require the following information also be included in the report:

    - the number of entities whose accreditation has been varied, suspended, and revoked;

[19] Bill, section 85.
[20] Bill, section 86.

- number of compliance assessments undertaken and number of failed compliance assessments.

Thank you again for the opportunity to comment on the draft digital ID legislation. I have no objection to this submission being published without further reference to me. I also propose to publish a copy of this submission on the OVIC website but would be happy to adjust the timing of this to allow you to collate and publish submissions proactively.

[redacted]

[redacted]