Australian Government

Office of the Australian Information Commissioner

2023 Digital ID Bill and Digital ID Rules – submission to the Department of Finance

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

17 October 2023

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the exposure drafts of the Digital ID Bill 2023 and Digital ID Rules 2024.

2. The 2023 Digital ID Bill (Bill) provides a legislative basis for the Australian Government Digital ID System (AGDIS) and for the phased expansion of the AGDIS to State, Territory and private-sector entities. The Bill also provides for an accreditation scheme for entities providing Digital ID services.

3. The OAIC is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act) and other legislation), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth) (FOI Act)), and information management functions (as set out in the *Information Commissioner Act 2010* (Cth)).

4. The OAIC has engaged with the Digital Transformation Agency (DTA) and Department of Finance (the Department) through the development of the Trusted Digital Identity Framework and has made submissions to three previous consultations on draft Digital Identity legislation.[1]

5. The OAIC is supportive of a legislative framework for Digital Identity and welcomes our proposed role as the independent privacy regulator for the scheme. We acknowledge that the Bill includes a number of strong privacy protections, particularly through the inclusion of additional privacy safeguards that will operate alongside existing protections under the Privacy Act. Robust privacy safeguards are fundamental to the effective functioning of the Digital ID system and to ensuring that individuals can have confidence that in using the system, their personal information will be protected.

6. At the same time, we consider that the Bill could be enhanced to provide greater clarity regarding the scope of the OAIC's role and our ability to effectively enforce privacy breaches in the Digital ID system. Ensuring that the Information Commissioner has appropriate oversight of the privacy aspects of the system and the ability to take enforcement action, where necessary, is crucial to ensuring that the personal information of Digital ID users is protected.

Regulatory arrangements

7. The Bill proposes a new Digital ID Regulator, which in the interim will be the ACCC. The Digital ID Regulator will have functions in respect of accreditation and approvals to participate in the AGDIS. The Information Commissioner will be responsible for regulating the privacy aspects of the Bill, including the additional privacy safeguards.

[1] OAIC, *Digital Identity Legislation Consultation Paper*, Submission to the Digital Transformation Agency, 18 December 2020; OAIC, *Digital Identity Legislation Position Paper*, Submission to the Digital Transformation Agency, 15 July 2021; OAIC, *Trusted Digital Identity Bill legislative package: exposure draft consultation*, Submission to the Digital Transformation Agency, 27 October 2021.

8. Under the Bill, State and Territory privacy authorities will also play a role in relation to State and Territory privacy legislation and the Digital ID Data Standards Chair will have responsibility for making technical standards for the AGDIS.

9. We understand that the Department has not yet finalised the division of regulatory functions between the Australian Competition and Consumer Commission (ACCC) as the Digital ID Regulator and Services Australia as administrator of the AGDIS. The OAIC notes that ensuring there is clarity about the remits of the system administrator and all regulators will be critical to building effective and wholistic oversight of the Digital ID system.

10. The OAIC looks forward to working with these other regulators to develop effective processes for information sharing and governance that promote cooperation and trust in the Digital ID scheme.

OAIC's jurisdiction

11. The Privacy Act and Chapter 3 of the Bill provide a legislative framework for the protection of personal information within the Digital ID system. The Bill requires all entities accredited under the Digital ID system to either:

- be subject to the Privacy Act;
- be subject to a State or Territory privacy law that provides for all of the following:
  - protection of personal information comparable to that provided by the Australian Privacy Principles (APPs);
  - monitoring of compliance with the law; and
  - a means for an individual to seek recourse if their personal information is dealt with in a way contrary to the law; or
- have entered into an 'APP-equivalent agreement' with the Commonwealth that requires compliance with the Australian Privacy Principles (APPs).[2]

12. Chapter 3, Part 2, Division 2 of the Bill sets out additional privacy safeguards which will operate in addition to the general protections under the Privacy Act. A contravention of these safeguards by any accredited entity will constitute an interference with the privacy of an individual for the purposes of the Privacy Act.[3] In enforcing the safeguards, the Information Commissioner will therefore have jurisdiction in respect of entities that may not otherwise fall within the scope of the Privacy Act, including State and Territory entities.

13. The Bill further expands the Information Commissioner's jurisdiction to include oversight of the privacy-related terms of an APP-equivalent agreement.[4] Additionally, the Bill extends the operation of the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act to

[2] Digital ID Bill, ^34

[3] Digital ID Bill, ^36.

[4] Digital ID Bill, ^35.

accredited entities that would not otherwise be covered by the Privacy Act or a comparable State or Territory scheme.[5]

14. The OAIC welcomes the additional privacy protections in the Bill and the proposed role of the Information Commissioner in respect of the Digital ID scheme. However, while we acknowledge that the Bill provides for privacy protections across the Digital ID system, we consider that there remains the potential for fragmentation in regulatory oversight. Under the proposed arrangements, some State and Territory entities will be required to comply with both State and Territory privacy legislation overseen by State and Territory regulators, and the additional privacy safeguards regulated by the OAIC.

15. The OAIC recommends consideration be given to whether greater consistency in privacy regulation could be achieved if accredited State and Territory entities were prescribed under s 6F of the Privacy Act in relation to their handling of personal information in the Digital ID system. Section 6F is a mechanism which allows the Governor-General to make regulations prescribing a State or Territory entity, so that the Privacy Act applies as if the entity were an organisation.

16. More broadly, the Government Response to the Privacy Act Review Report[6] has given in-principle agreement to establish a Commonwealth, State and Territory working group to harmonise privacy laws, focusing on key issues (Proposal 29.3). The Digital ID system and other initiatives of national significance would benefit from this type of working group, noting that State and Territory governments are increasingly working together on national initiatives that involve sharing information across jurisdictions and that greater harmonisation could reduce the compliance burden on entities.

Recommendation 1. Consider whether greater consistency in privacy regulation could be achieved if accredited State and Territory entities were prescribed under s 6F of the Privacy Act.

APP-equivalent agreements

17. The OAIC acknowledges that the 'APP-equivalent agreement' appears to be based on a similar concept from the *Data Availability and Transparency Act 2022* (Cth) (DAT Act), which provides for 'APP-equivalence terms' of data sharing agreements.

18. We note that there is currently limited information regarding the intended scope of these agreements and the Bill does not place limits around the types of entities which can enter into such an agreement.

19. For clarity, the Bill should explicitly limit APP-equivalent agreements to accredited State and Territory entities. The Bill should further specify that private sector entities which are not considered organisations under the Privacy Act be required to opt-in to coverage under s 6EA of the Privacy Act. Section 6EA provides an established process with greater regulatory certainty for

[5] Digital ID Bill, ^38.

[6] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 13 October 2023, pp 300-303; AGD, *Privacy Act Review – Government Response*, AGD, September 2023, accessed 13 October 2023, p 34.

private sector entities seeking Privacy Act coverage, ensuring that breaches can be effectively enforced.

20. The OAIC also suggests that APP-equivalent agreements be required to be registered as legislative instruments. This would provide greater clarity and transparency in ensuring that accredited non-APP entities are subject to the Privacy Act and APPs.

21. Alternatively, if the Department proceeds with the use of APP-equivalent agreements which are not legislative instruments, we recommend amendments to the Bill to ensure the Information Commissioner is provided with a copy of all such agreements. This is necessary for ensuring that the OAIC is aware of the entities which are subject to such agreements and can efficiently enforce any privacy breaches. We also recommend that APP-equivalent agreements should be published in the interests of transparency and clarity to participants engaging with the AGDIS.

Recommendation 2. Explicitly limit APP-equivalent agreements to accredited State and Territory entities and require private-sector entities to opt-in to Privacy Act coverage under s 6EA of the Privacy Act.

Recommendation 3. APP-equivalent agreements should be required to be registered as legislative instruments. Alternatively, amend the Bill to require the Minister to notify the Information Commissioner when entering into an APP-equivalent agreement under ^32 and provide a copy of the agreement and also publish the agreement.

Comparable State and Territory laws

22. The Bill specifies criteria that a State or Territory privacy law must meet in order for State and Territory accredited entities to do an act or engage in a practice with respect to personal information under the Digital ID scheme.[7] This includes a requirement that the law offer a level of protection of personal information comparable to that provided by the APPs. Similarly, accredited State and Territory entities will be required to comply with Notifiable Data Breach scheme requirements under Part IIIC of the Privacy Act unless they are covered by a comparable State or Territory scheme.[8]

23. The Bill does not appear to contain a mechanism or process for formally assessing equivalency of State and Territory privacy laws and does not specify who will be responsible for the assessment. We note however that in assessing an application for accreditation the Digital ID Regulator is required to consider the applicant's ability to comply with the Digital ID Act and Rules if accredited.[9] This would most likely include an assessment of whether the applicant is subject to legal obligations in respect of privacy, as required by clause 34.

24. The OAIC queries whether the Digital ID Regulator will be appropriately equipped to undertake equivalency assessments. More broadly, the OAIC encourages the Department to amend the Bill to

[7] Digital ID Bill, ^34(2)(b).

[8] Digital ID Bill, ^38(2) and ^39.

[9] Digital ID Bill, ^15(4); Digital ID Accreditation Rules, ^2.7.

include a clear mechanism for determining whether a State or Territory privacy law meets the criteria in clauses 34(2)(b) and 38(2)(b). Incorporating an express mechanism in the Bill will help to ensure clarity for both accredited entities and regulators as to the applicable privacy law.

25. One example of an express mechanism is in the *My Health Records Act 2012*, which provides for the Minister to determine a State or Territory law to be a 'designated privacy law'.[10] We note that an advantage of this process is that it provides for equivalency to be determined at the State/Territory level, rather than requiring each entity to provide evidence of equivalency in an accreditation application. We note that it may not be feasible for the Digital ID Regulator to assess equivalency on an entity-by-entity basis.

Recommendation 4. Amend the Bill to clarify the responsible body, and the process, for determining whether a State or Territory privacy law meets the criteria in clauses 34(2)(b) and 38(2)(b).

De-identification or destruction of personal information

26. Clause 130 sets out requirements for the destruction or de-identification of personal information that was obtained through the AGDIS by an accredited entity, if:

    a. the entity is not required or authorised to retain the information by law or under a court/tribunal order; and

    b. the information does not relate to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity is a party.

27. As discussed in a previous submission, the OAIC is of the view that clause 130 is an important element of the privacy protective framework, and is similar to the requirement in APP 11.2 for APP entities to take reasonable steps to destroy or de-identify information that is no longer required for a purpose for which it may be used or disclosed under the APPs.[11]

28. Given the potential regulatory overlap between clause 130 and APP 11.2, the OAIC recommends that the requirement in clause 130 is included as an additional privacy safeguard, and regulated by the Information Commissioner. This would remove the risk of inconsistent interpretations of an entity's destruction or de-identification obligations by the Digital ID Regulator and the Information Commissioner, and provide greater clarity for accredited entities.

29. The OAIC also encourages the Department to consider whether clause 130 could also provide for greater specificity regarding retention periods. Without clear retention periods, there is an increased risk that individuals' personal information will be held for longer than is necessary and become compromised in the event of a data security incident. The Government has recognised

[10] *My Health Records Act 2012*, section 110.

[11] OAIC, *Trusted Digital Identity Bill legislative package: exposure draft consultation*, Submission to the Digital Transformation Agency, 27 October 2021.

these risks in the Government Response to the Privacy Act Review Report,[12] which agrees in-principle with the recommendation that the Commonwealth undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information (Proposal 21.6).

30. The OAIC considers that the current drafting of clause 130 may lack the necessary degree of certainty to ensure data security risks are effectively mitigated, particularly because the clause defers to other laws and court/tribunal orders for retention requirements. The OAIC recommends that consideration is given to clearly specifying a set timeframe for the retention of personal information.

Recommendation 5. Amend the Bill to make the destruction and de-identification requirement in clause 130 an additional privacy safeguard in Chapter 3, Part 2, Division 2.

Recommendation 6. Consider whether clause 130 could provide greater specificity regarding retention of personal information.

Scope of the Rules

31. The proposed Digital ID regulatory framework provides for significant detail to be included in the Accreditation Rules and Digital ID Rules. This includes matters relating to the handling of personal information. By way of example, the Bill states the Accreditation Rules may:

    a. Deal with matters including requirements relating to the collection, holding, use and disclosure of personal information of individuals;[13]

    b. Provide for and in relation to the collection, use, disclosure, storage or destruction of biometric information by accredited entities;[14] and

    c. Authorise accredited entities to collect or disclose restricted attributes.[15]

32. The OAIC's general preference is that privacy protections be embedded in primary legislation. We also appreciate the need for flexibility as part of the regulation of major technology initiatives, which are subject to phased expansion.

33. However, given the nature of personal and sensitive information that will be handled under the proposed Accreditation Rules, it should be clear under the draft Bill that the Information Commissioner will have the power to enforce privacy protections in the Rules. We are concerned that without this certainty, the OAIC's capacity to effectively regulate the privacy aspects of the Digital ID scheme may be limited. We recommend that further consideration be given to ensuring

[12] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 13 October 2023, pp 225-227; AGD, *Privacy Act Review – Government Response*, AGD, September 2023, accessed 13 October 2023, pp 36.

[13] Digital ID Bill, ^27(2)(g)

[14] Digital ID Bill, ^49

[15] Digital ID Bill, ^18(6) and (7), ^19.

that the Commissioner's regulatory role extends to the privacy aspects of the Rules, to further mitigate privacy risks in the system.

Recommendation 7. Amend the Bill to expressly provide for the Information Commissioner's jurisdiction in respect of privacy protections in the Rules.