Australian Government

Office of the Australian Information Commissioner

Exposure Draft – Trusted Digital Identity Bill 2021 legislative package

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

27 October 2021

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the legislative package for Digital Identity, which includes exposure drafts for the Trusted Digital Identity Bill 2021 (TDI Bill), Trusted Digital Identity Framework Accreditation Rules 20xx (TDIF Rules) and Trusted Digital Identity Rules 20xx (TDI Rules) (together, the legislative package). A plain English explanation of Digital Identity and a Regulatory Impact Statement accompany the legislative package.[1]

2. The OAIC has engaged with the DTA over several years as they developed the Trusted Digital Identity Framework (TDIF). Most recently, we have participated as a member of the Digital Identity and MyGov Steering Committee, and as an observer on an interdepartmental committee to develop the legislation for the system. The OAIC also made submissions to the DTA's two previous consultation papers on Digital Identity legislation.[2]

3. Digital identity is a key part of the government's Digital Economy Strategy, aiming to provide 'secure and simple access to services from government and across the economy.'[3] The legislative package enshrines the TDIF in law, providing a standard that can be used by other digital identity systems and also creates the government's Trusted Digital Identity System (TDIS). Given its role in laying the groundwork for future digital identification systems, it is crucial to get the regulatory settings right.

4. The OAIC welcomes its proposed role as the independent privacy regulator for the TDIF and the TDIS and additional privacy safeguards being enshrined in law. Strong privacy protections and robust regulatory oversight are critical to building trust in digital identity systems. The results of the OAIC's 2020 Australian Community Attitudes to Privacy Survey show that identity theft and fraud are the biggest perceived risks to privacy for Australians.[4] The survey also found that Australians are cautious around collection of biometric information to verify their identity to access services provided by a government service (53% comfortable with this use) or business or private organisation (only 33% comfortable with this use).[5] Trust in how personal information is handled and protected is therefore essential to build community confidence and increase the uptake of digital identity.[6]

5. With this in mind, this submission considers what further protections should be included in the legislation to promote the integrity of the TDIF and the TDIS and individual choice over when and how personal information is handled. Clarity about the obligations on entities and when

---

[1] Under the *Privacy Act 1988* (Cth) (Privacy Act), one function of the Privacy Commissioner is to examine proposed enactments that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals. The Commissioner also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised. See s 28A of the Privacy Act.

[2] OAIC (2020), Digital Identity Legislation Consultation Paper – Submission to the Digital Transformation Agency; OAIC (2021), Digital Identity Legislation Position Paper – Submission to the Digital Transformation Agency.

[3] Australian Government, Digital Economy Strategy 2030, p 2.

[4] OAIC (2020), *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, pp 105-106.

[5] OAIC (2020), *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, pp 83-84.

[6] See DTA (2021), *Regulation Impact Statement: Regulation of the Australian Government Digital Identity System*, pp 27-28.

they apply, together with appropriate proactive and reactive enforcement mechanisms, will be essential to success of the TDIF and the TDIS.

6. The OAIC looks forward to continuing to engage with the DTA on appropriate protections within digital identity and the establishment of the co-regulatory model.

Privacy protections in the legislative package

7. The *Privacy Act 1988* (Cth) (Privacy Act) and Chapter 4 of the TDI Bill provide a legislative framework for the protection of personal information that flows through accredited digital identity facilities.[7] The TDI Bill promotes a consistent level of privacy protection by requiring all entities accredited under the TDIF (accredited entities) to either:
    - be APP entities under the Privacy Act
    - be covered by a State or Territory privacy law that meets criteria set out in the TDI Bill
    - have a trusted provider agreement that requires compliance with the APPs.[8]
8. In addition, the TDI Bill applies the notifiable data breach (NDB) scheme in Part IIIC of the Privacy Act to entities that are not APP entities and are not covered by a State or Territory law that is comparable to the NDB scheme.[9]
9. The legislative package contains additional restrictions on how personal information can be collected, used and disclosed by entities under the TDIF. Chapter 4 Part 2 Division 2 of the TDI Bill contains additional privacy safeguards, including a requirement to obtain the individual's express consent before sending their attributes to a relying party when verifying or authenticating an individual, restrictions on biometric information and some restrictions on use and disclosure of digital identity information.[10] The TDIF Rules contain further protections, including strict restrictions on what attributes accredited identity service providers can collect and when they can disclose restricted attributes.[11]
10. The OAIC welcomes these additional privacy protections, which introduce important restrictions on the handling of personal information. These privacy protections apply to all accredited entities, whether they are onboarded to the TDIS or not, although enforcement

[7] The accredited facility of an entity means the facility through which the entity provides the services for which the entity is accredited. See Trusted Digital Identity Bill 2021 (Cth) s 9 (definition of accredited facility).

[8] Trusted Digital Identity Bill 2021 (Cth) s 65.

[9] Trusted Digital Identity Bill 2021 (Cth) s 68.

[10] Digital identity information means information that is generated in a digital identity system, obtained from a digital identity system or collected for the purposes of a digital identity system. See Trusted Digital Identity Bill 2021 (Cth) s 9 (definition of digital identity information).

[11] An attribute of an individual means information that is associated with the individual and includes information that is derived from another attribute but is not biometric information of an individual, a restricted attribute of an individual, certain types of sensitive information or information prescribed by the TDI Rules. For the full definition see the Trusted Digital Identity Bill 2021 (Cth) s 10. A restricted attribute of an individual means health information about the individual, an identifier of the individual issued or assigned by or on behalf of the Commonwealth, a State or a Territory itself or their authority or agency, or information prescribed by the TDI Rules. For the full definition see the Trusted Digital Identity Bill 2021 (Cth) s 11.

mechanisms differ. Uniform application of privacy protections is key to the integrity of the TDIF, and it is important that the DTA ensures that different levels of accreditation do not create or increase privacy risks that are unable to be appropriately mitigated as digital identity progresses.

11. The OAIC also welcomes the proposed role of the Information Commissioner as regulator of the privacy requirements under the legislation. The legislative package creates a co-regulatory model between the Information Commissioner and the Oversight Authority. State and Territory privacy authorities also play a role in relation to State and Territory privacy legislation. The OAIC looks forward to working with these other regulators to develop effective information sharing and governance mechanisms that promote cooperation and trust in the TDIF.

12. The new privacy protections and expansion of entities subject to the APPs and NDB scheme expand the regulatory jurisdiction of the OAIC. The OAIC will need appropriate resourcing to properly carry out its statutory functions as independent privacy regulator of the TDIF and TDIS.

Strengthening the privacy-protective framework

13. While the OAIC supports the privacy protections already contained in the legislative package, we recommend that the DTA include additional key privacy protective measures to further mitigate privacy risks and promote trust in the TDIF.

Strong consent requirements

14. One of the additional privacy safeguards created by the TDI Bill is to require an individual's express consent to send their attributes or restricted attributes to a relying party when verifying or authenticating an individual.[12] This is an important mechanism to ensure individuals retain control of their digital identity and attributes.

15. Currently, the TDIF Rules contain further requirements for express consent, including requiring an individual's express consent to use or disclose their attributes or restricted attributes to verify them with an attribute verification service or authoritative source.[13] The TDIF Rules also set out requirements for a straightforward process to withdraw consent, obtaining enduring consent, and keeping records of consent.[14]

16. The OAIC recommends that these requirements are included in the TDI Bill, given the importance of consent within the TDIF and the TDIS. Where possible, privacy requirements should be included in primary legislation to guard against inadvertent or unforeseen risks to privacy, such as the collection, use or disclosure of personal information that may not have been originally intended, known as 'function creep', or that which may not be reasonable, necessary and proportionate to the relevant policy objectives.

[12] Trusted Digital Identity Bill 2021 (Cth) s 73-74.

[13] *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth)Chapter 4, Part 3, r 3.9(2).

[14] *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 4, Part 3, r 3.9(3)-(5)

17. We also recommend additional requirements be introduced to the TDI Bill to strengthen the standard of consent and align the standard with that in the Consumer Data Right (CDR).[15] In particular, the additional requirements in the CDR that consent is voluntary, informed, specific as to purpose and time limited should be incorporated into the TDI Bill.[16]

18. Finally, the OAIC recommends that the TDI Bill explicitly limits the maximum duration of an enduring consent to disclosure of attributes to 12 months. This provides clarity about the need for consent to be time limited in the context of digital identity and is consistent with the requirements under the CDR.[17]

19. Guidance should also be developed to provide further detail on how accredited entities can satisfy express consent requirements.

Recommendation 1: Include all requirements relating to the standard and seeking of consent in the TDI Bill.

Recommendation 2: Align requirements for consent with those in the CDR such that consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

Recommendation 3: Limit enduring consents to a maximum duration of 12 months.

Limiting use and disclosure of digital identity information

20. Given the nature of the personal and sensitive information that will be held by accredited entities, the OAIC considers the legislation should clearly set out the purposes for which personal information that is digital identity information can be used or disclosed.

21. We are supportive of the existing provisions in the legislative package that limit the use and disclosure of digital identity information. For example, accredited entities cannot use or disclose certain kinds of digital identity information unless it is for narrow authorised purposes set out in s 80 of the TDI Bill.[18] These purposes relate to providing the services for which the entity is accredited and complying with law.[19] In addition, the legislation only permits limited disclosure of digital identity information for law enforcement purposes and prohibits use or disclosure for marketing purposes.[20] As set out above, accredited entities must also have express consent to disclose attributes to relying parties and there are strict requirements regarding biometrics.[21]

---

[15] See *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 4.9.

[16] We note the legislative package already contains requirements for consent to be express and easily withdrawn.

[17] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 4.12(1).

[18] The kinds of information this restriction applies to are information about the services provided by the entity that an individual has accessed or attempted to access, information relating to how or when access was obtained or attempted, information relating to the method of access or attempted access, or the date and time the individual's identity was verified. See Trusted Digital Identity Bill 2021 (Cth) s 80(1).

[19] Trusted Digital Identity Bill 2021 (Cth) s 80(2).

[20] Trusted Digital Identity Bill 2021 (Cth) ss 81-82.

[21] Trusted Digital Identity Bill 2021 (Cth) ss 73-73, 76-79.

22. However, we note that the TDIF Rules also require entities to have user terms in place that are likely to provide further information about the primary and secondary purposes for which digital identity information will be used or disclosed.[22] These user terms may further expand the permitted uses or disclosures of digital identity information.

23. This approach differs to the restrictions under the CDR and My Health Record (MHR) legislation, which provide a strong level of protection by prohibiting the use and disclosure of CDR data and health information in a MHR, except for narrow authorised purposes in the legislation.[23]

24. In line with this approach, the OAIC recommends that the TDI Bill is amended to adopt the restrictions in s 80 in relation to all digital identity information. This would set a uniform standard of protection for personal information under the TDIF, rather than relying on the individual user terms of accredited entities. Importantly, it would reduce the ability of accredited entities to use information for unexpected purposes on the basis of purported consent obtained through the user terms of the accredited entity. In addition to reducing the burden on individuals to carefully read and understand complicated data handling terms and conditions, this would assist regulated entities to understand how they can use or disclosure digital identity information in a way that promotes trust in their services.

Recommendation 4: Amend s 80 of the TDI Bill to prohibit the use or disclosure of any digital identity information held in an entity's accredited facility, except as permitted under subsection 80(2).

Law enforcement access to digital identity information

25. The current drafting of the TDI Bill limits law enforcement access to digital identity information to use or disclosure for the purposes of enforcement related activities conducted by or on behalf of an enforcement body where:

    - the enforcement body reasonably suspect a person has committed an offence, breached a law or has started proceedings for an offence or breach of law, or
    - the use or disclosure is pursuant to a warrant.[24]

26. In addition, the TDI Bill prohibits law enforcement access to biometric information, even where an enforcement body has a warrant, authorisation or order issues under a law.[25]

27. Given the importance of building and maintaining trust in the TDIF to encourage uptake of digital identity, the OAIC strongly recommends that law enforcement access to digital identity information that is not biometric information is limited further, to only permit law enforcement access where necessary to address misuse or fraud within the digital identity system, or

[22] *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 5, Part 2, r 2.1.

[23] See for example, *My Health Records Act 2012* (Cth) s 59, *Competition and Consumer Act 2010* (Cth) s 56EI.

[24] Trusted Digital Identity Bill 2021 (Cth) s 81.

[25] Trusted Digital Identity Bill 2021 (Cth) s 76(2)-(3).

pursuant to a warrant. This will help to ensure that law enforcement is only permitted where reasonable, necessary and proportionate to achieve a legitimate aim.

28. As demonstrated by recent community concerns about law enforcement access in the context of COVID-19 check-in apps, appropriate limits on law enforcement access are important from a public policy perspective to encourage uptake of new systems.[26] There are justifiable policy reasons for law enforcement access relating to serious misuse of a digital identity system and fraud prevention. In these circumstances law enforcement may play a role in creating a trusted and secure system through policing misuse. In contrast, any access rights beyond these circumstances, such as to protect public revenue, must be carefully scrutinised. Requiring a warrant to access information provides a pertinent level of judicial oversight.[27]

29. We also note the important role of the annual transparency report requirement for identity exchanges under the TDIF Rules. This requirement promotes transparency of the number of requests enforcement bodies make to identity service provider for access to digital identity information. Given its importance we recommend it be included in the primary legislation and extended to all accredited service providers.

Recommendation 5: Amend s 81 so that law enforcement access is limited to what is necessary to address misuse of or fraud in a digital identity system.

Recommendation 6: Include the requirement for an annual transparency report requirement in primary legislation and extend this requirement to all accredited service providers.

Limiting the disclosure of restricted attributes

30. A 'restricted attribute of an individual' is health information about the individual, identifiers issued by or on behalf of the Commonwealth, a State or a Territory and any information that is prescribed by the TDI Rules and relates to the individual.[28] The first two categories of restricted attributes are already subject to extra protections under the Privacy Act through protections for sensitive information and government-related identifiers respectively.[29]

31. Given the sensitivity of this information, it is important to ensure they are appropriately protected within the TDIF and the TDIS. The legislative package currently does this by requiring Oversight Authority authorisation for identity service providers to disclose restricted attributes to third parties and for onboarded accredited entities, including participating relying parties, to

[26] See for example Kenith Png, 'Police would not agree to stop accessing COVID SafeWA app data, Premier Mark McGowan says', *ABC News*, accessed 20 October 2021.

[27] Under the Consumer Data Right, law enforcement access under APP 6 is not permitted. Instead, access must be required or authorised by or under an Australian law, or a court/tribunal order. See *Competition and Consumer Act 2010* (Cth) s 56EI.

[28] Trusted Digital Identity Bill 2021 (Cth) s 12.

[29] See, for example, specific protections for sensitive information in *Privacy Act 1988* (Cth) APPs 3 and 6, and protections for government-related identifiers in APP 9.

obtain and disclose restricted attributes.[30] This authorisation is by way of imposing a condition that allows the entity to disclose or receive restricted attributes.[31]

32. The OAIC recommends that further detail is provided in the legislative package about the authorisation process for identity service providers. In particular, the TDIF Rules should contain information about the scope of the authorisation that can be granted by the Oversight Authority and the factors the Oversight Authority will consider in deciding to grant an authorisation. For example, the Oversight Authority should be required to consider whether the proposed use or disclosure of a restricted attribute is reasonable, necessary and proportionate to achieving a legitimate policy aim. This is an important consideration given the Oversight Authority's authorisation to disclose restricted attributes may engage required or authorised by law exceptions under the Privacy Act.[32]

33. The OAIC also recommends that additional protections are introduced to ensure authorisations for participating relying parties to receive restricted attributes are only granted where appropriate. The conditions in s 23(2) of the TDI Bill for the Oversight Authority to consider in deciding whether to authorise the participating relying party to receive restricted attributes should be expanded to include additional considerations to determine whether the authorisation is reasonable, necessary and proportionate.

Recommendation 7: Amend rule 3.7 of Chapter 5 Part 3 of the TDIF Rules to include detail on:

- the scope of the authorisation, in particular, the duration of the authorisation and whether the authorisation permits the identity service provider to disclose all restricted attributes to all third parties or only specified restricted attributes to specified third parties
- the factors that the Oversight Authority will consider in deciding to grant authorisation.

Recommendation 8: Amend s 23(2) of the TDI Bill to require the participating relying party to:

- justify the reason for requesting the attributes
- demonstrate why a similar result cannot be achieved without the proposed sharing of restricted attributes
- describe data flows showing how the restricted attributes will be used
- demonstrate how the relying party meets any other legislative or regulatory requirements applicable to the restricted attribute.

[30] Trusted Digital Identity Bill 2021 (Cth) ss 22-23; *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 5 Part 3, r 3.7(2). A participating relying party is a relying party that is onboarded onto the TDIS. See Trusted Digital Identity Bill 2021 (Cth) s 9 (definition of participating relying party).

[31] Trusted Digital Identity Bill 2021 (Cth) ss 22-23; *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 5 Part 3r 3.7(2).

[32] *Privacy Act 1988* (Cth) APP 9.2(c).

Disclosures between participating relying parties and other relying parties

34. The TDI Rules prohibit participating relying parties from disclosing attributes and restricted attributes of an individual to another relying party unless permitted by a condition of the participating relying party's approval.[33]

35. The OAIC support this prohibition and recommend it is extended to prohibit disclosures to any third party. This will further strengthen the integrity of the TDIS as it clearly establishes that personal information in the TDIS is not intended to be transferred outside of the TDIS unless permitted by a condition of approval.

36. We also recommend that the TDI Bill is amended to include strict limits on when the Oversight Authority will grant this condition as part of a participating relying party's approval. Allowing a participating relying party to disclose attributes and restricted attributes to entities that are not onboarded takes the personal information outside of the protective framework created by the legislative package. This should only occur in limited circumstances and further consideration should be given to the protections that will apply to personal information that has been disclosed in these circumstances.[34]

Recommendation 9: Prohibit participating relying parties from disclosing attributes and restricted attributes to any entity, unless authorised by the Oversight Authority.

Recommendation 10: Amend the TDI Bill to include strict limits on when authorisation by the Oversight Authority will be granted and consider what protections for personal information could be introduced to maintain the level of protection when participating relying parties provide information collected through the TDIS to third parties, including relying parties.

Protections for biometric information

37. The legislative package includes protections for biometric information in the additional privacy safeguards and the role requirements for identity service providers and credential service providers in the TDIF Rules.[35]

[33] A participating relying party is a relying party that is onboarded onto the TDIS. See Trusted Digital Identity Bill 2021 (Cth) s 9 (definition of participating relying party).

[34] To onboard to the system, participating relying parties are required to meet the fit and proper person test and once onboarded they have certain notification and redress obligations that will not apply to other relying parties – see Trusted Digital Identity Bill 2021 (Cth) s 18; *Trusted Digital Identity Rules 202x* (Cth). Relying parties that have not onboarded to the system (i.e. that are not participating relying parties) are not subject to these requirements.

[35] Trusted Digital Identity Bill 2021 (Cth) ss 76-79; *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 5, Part 3, r 3.8-3.9, Chapter 5, Part 4, r 4,3.3 . We understand the requirements in the TDIF Rules are being revised.

Defining and limiting biometric information

38. 'Biometric information of an individual' means information about any measurable biological characteristic relating to an individual that could be used to identify the individual or verify the individual's identity and includes biometric templates.[36] The OAIC recommends that this definition be amended to include 'behavioural characteristics', which more closely aligns with existing definitions of biometric information, such as in the Department of Home Affairs' National Identity Proofing Guidelines.[37].

39. The definition proposed in the TDI Bill also captures a broad range of biometrics, each of which may carry different privacy risks and requirements as to what process is required for biometric binding. For example, the current biometric requirements in the TDIF Rules for identity services providers appear directed towards face verification.[38] We recommend that the TDI Bill prohibits accredited entities using biometric information of an individual unless it is a kind of biometric information included on a list in the TDIF Rules. This will ensure that any additional privacy protections and procedural mechanisms required for use of biometric information that was not previously contemplated can be put in place.

One-to-one matching

40. The OAIC recommends that the prohibition of one-to-many matching is elevated from the TDIF Rules into primary legislation.[39] The prohibition on one-to-many matching and requirement for one-to-one matching for biometrics is an important part of the privacy protective regime for biometrics. One-to-many biometric matching is a process in which biometric information is compared to a database of individuals to locate a positive match. In contrast one-to-one matching is the comparison of biometric information against a known biometric template or stored image of the individual. This means that unlike one-to-many matching, one-to-one matching does not require ongoing access to a database containing personal information.

Deletion of biometric information

41. Another important protection is s 79 of the TDI Bill which requires deletion of biometric information. The OAIC recommends that this is amended to require the destruction of biometric information. As set out in our guide to securing personal information, personal information is destroyed when it can no longer be retrieved.[40] Given the sensitivity of biometric information, this is an appropriate standard to set for the protection of this information.

Recommendation 11: Amend the definition of biometric information to include 'behavioural characteristics'.

[36] Trusted Digital Identity Bill 2021 (Cth) s 9 (definition of biometric information of an individual).

[37] Home Affairs, National Identity Proofing Guidelines, p 24.

[38] See *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 5, Part 3, r 3.8-3.9.3.

[39] *Trusted Digital Identity Framework Accreditation Rules 202x* (Cth) Chapter 5, Part 3, r 3.8.3(3)-(4).

[40] OAIC (June 2018), Guide to securing personal information [online document], OAIC website, accessed 13 October 2021.

Recommendation 12: Prohibit the use or disclosure of biometric information of an individual within digital identity, unless it is a kind of biometric information listed in the TDIF Rules.

Recommendation 13: Elevate the prohibition on one-to-many matching and the requirement for one-to-one matching into the TDI Bill.

Recommendation 14: Amend s 79 of the TDI Bill to require destruction of biometric information instead of deletion of biometric information.

Retaining appropriate protections for testing

42. Sections 37 and 38 of the TDI Bill allow use or disclosure of personal information for the purposes of conducting testing to determine an entity's capability or suitability to onboard to the trusted digital identity system. This is permitted to occur where the entity holds an authorisation from the Oversight Authority and the individual to whom the information relates has expressly consented to the use or disclosure of the information for that purpose.

43. The OAIC recommends that additional privacy protections should be put in place to limit the burden on individuals of having to understand the implications of consenting to the handling of their personal information for this purpose.

44. The OAIC is concerned that the testing provisions apply despite anything else in the TDI Bill, including the additional privacy safeguards, which were developed in recognition of the sensitivity of digital identity information. In addition, as the entity conducting the testing is not required to be accredited they may not be subject to the Privacy Act or equivalent State or Territory legislation.

45. This differs significantly from the approach under the CDR legislative framework, where CDR data recipients must be accredited before they receive access to the Conformance Test Suite (CTS) and the CTS does not involve any consumer data.[41]

46. We are not clear why using a test environment that uses synthetic information instead of personal information is not technically feasible or would place a disproportionate burden on the effective functioning of the TDIS. Given CDR does not use consumer data (which includes personal information) as set out above, we suggest the DTA consider how to align with the CDR approach.

47. A privacy impact assessment (PIA) may assist the DTA to fully consider the impact the testing mechanisms under ss 37 and 38 of the TDI Bill may have on privacy and how to manage, minimise or eliminate that impact. We recommend the DTA conduct a PIA considering issues such as:

    - how to meet the objectives of these provisions through other means that are less privacy intrusive without the use of personal information

[41] See ACCC (17 March 2021), *Consumer data right: CDR Conformance Test Suite*, ACCC website, accessed 19 October 2021.

- if consent is required, how consent can be truly voluntary, informed, time limited, easily withdrawn and specific as to purpose, and given by a person with the capacity to provide consent
- the privacy impacts of entities not subject to the Privacy Act receiving access to personal information and the extent that this can be managed or mitigated
- the extent to which any other privacy risks and foreseeable future privacy risks stemming from these provision can be managed or mitigated through the implementation of appropriate policies, procedures and privacy controls.

Recommendation 15: Undertake a PIA to determine whether the proposed testing mechanism is reasonable, necessary and proportionate, including consideration of the issues set out above.

Destruction or de-identification of personal information

48. The OAIC considers that s 132 of the TDI Bill is an important element of the privacy protective framework, requiring certain accredited entities to destroy or de-identify personal information that was obtained through the trusted digital identity system that:[42]
    - the entity is not required to retain under the legislative package, another law or a court or tribunal order
    - does not relate to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity is a party.
49. This requirement 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. A decision about whether an APP entity that is covered by s 132 of the TDI Bill has taken reasonable steps under APP 11.2 will likely need to consider the entity's destruction/de-identification obligations under the TDI Bill.
50. The OAIC recommends that the TDI Bill is amended to make the requirements of s 132 an additional privacy protection in Chapter 4, Part 2, Division 2, given the potential regulatory overlap with APP 11. This would ensure that the requirement is an interference with privacy and the Information Commissioner has regulatory oversight through the mechanism in s 66 of the TDI Bill.
51. The OAIC considers that this is an important amendment to remove the risk of inconsistent interpretations of an entity's destruction or de-identification obligations by the Oversight Authority and the Information Commissioner. This will provide greater clarity to individuals and regulated entities about the interaction between the TDI Bill and the Privacy Act and their rights and obligations under each.

[42] This provision only applies to accredited and onboarded entities and accredited entities whose approval to onboard has been suspended or revoked. See Trusted Digital Identity Bill 2021 (Cth) s 132.

52. The OAIC also recommends that the destruction requirements under the TDIF and TDIS are strengthened by requiring TDIF accredited entities to have a data retention policy that reflects APP 11.2 as part of the documentary requirements that they must fulfill under the TDIF Rules.

Recommendation 16: Amend the TDI Bill to make the destruction and de-identification requirement s 132 an additional privacy safeguard in Chapter 4, Part 2, Division 2.

Recommendation 17: Include a requirement in the TDIF Rules for entities to have a data retention policy that reflects APP 11.2.

Offboarding

53. Section 61 of the TDI Bill requires an accredited service provider to deactivate a digital identity on request of the individual. However, the legislative package does not set out a clear process for offboarding of entities when they wish to exit the TDIS or the TDIF or their approval to onboard or accreditation is revoked. The position paper states that in these situations the Oversight Authority would give directions to the accredited entity to facilitate offboarding, such as requiring the accredited entity to notify individuals of their offboarding.[43]

54. When an accredited entity offboards it will be important for relevant individuals to be notified and for there to be specific requirements about the treatment of personal information that do not place an excessive burden on the individual user. We recommend the DTA consider how these outcomes can be achieved, such as through a formalised offboarding process or minimum legislative standards about the privacy protective directions that can be issued.

Recommendation 18: Consider how notification to the individual and appropriate mechanisms for the treatment of personal information can be built into offboarding.

Maintaining a voluntary system

55. The guide to digital identity provided with the legislative package states that creation and use of a digital identity under the TDIS will be voluntary.[44] The TDI Bill prohibits a participating relying party from requiring individuals to generate or use a digital identity to access its services unless a Commonwealth, State or Territory law requires verification solely by means of a digital identity, the relying party holds an exemption from the Oversight Authority or the participating relying party is of a kind covered by the TDI Rules.[45] The TDI Bill places important limits on when the Oversight Authority can grant an exemption, requiring it to be satisfied that it is appropriate to grant an exemption and prohibiting it from granting an exemption to relying parties that

[43] DTA (June 2021), 6 Governance of the Digital Identity system, *Digital Identity Legislation Position Paper*, 6.6.

[44] DTA (October 2021), *Your guide to the Digital Identity legislation*, p 28.

[45] Trusted Digital Identity Bill 2021 (Cth) s 30.

provide an essential service, are the sole provider of a service or access to services of a particular kind, or where it is otherwise in the public interest to refuse to grant an exemption.[46]

56. The OAIC notes these requirements are designed to ensure that individuals have a choice about whether engage with the DI system. The existence of a viable alternative may influence whether consent is freely given. As such, it is important that the exceptions to this prohibition are strictly limited and that the Oversight Authority only grant exemptions in narrow circumstances.

57. The OAIC recommends that additional requirements are included in the TDI Bill to further support the voluntary system:

- The Minister should be required to have regard to the same considerations as the Oversight Authority when deciding whether to make TDI Rules specifying that a kind of participating relying party does not need to comply with this requirement. The OAIC considers that this is necessary given subordinate legislation is not subject to the same level of scrutiny as primary legislation.
- Additional clarification should be provided on the threshold to be met before the Oversight Authority is satisfied it is appropriate to grant an exemption. This is particularly important in relation to the consideration that it may be appropriate to grant an exemption if the participating relying party is a small business (within the meaning of the Privacy Act).[47] This would represent a significant proportion of the businesses currently operating in Australia. As at 30 June 2019, small businesses with a turnover of $3 million or less comprised 95.2% of the 2,375,753 businesses actively trading in the Australian economy.[48]
- The TDI Bill should include civil penalties for breach of the prohibition on relying parties requiring individuals to generate or use a digital identity to access its services. Effective enforcement mechanisms are essential to promoting compliance by regulated entities and are justified here given the importance of choice.

Recommendation 19: Amend the TDI Bill to require the Minister to have regard to the same considerations as the Oversight Authority before specifying in the TDI Rules that a kind of participating relying party is not subject to the prohibition on relying parties requiring individuals to generate or use a digital identity to access its services.

Recommendation 20: Include additional requirements in the TDI Bill for the Oversight Authority to be satisfied it is appropriate to grant an exemption to the prohibition on relying parties requiring individuals to generate or use a digital identity to access its services.

Recommendation 21: Include civil penalties in the TDI Bill for breach of the prohibition on relying parties requiring individuals to generate or use a digital identity to access its services.

[46] Trusted Digital Identity Bill 2021 (Cth) s 30(3)-(5).

[47] Trusted Digital Identity Bill 2021 (Cth) s 30(4).

[48] Australian Bureau of Statistics, 8165.0 Counts of Australian Businesses, including Entries and Exits, Jun 2015 to Jun 2019, prepared for the OAIC in April 2020.

Clear and consistent obligations for regulated entities

Future-proofing for a changing Privacy Act

58. We note that the Attorney-General's Department is currently conducting a review of the Privacy Act.[49] Alignment between privacy obligations is essential to promote clarity for individuals and regulated entities. We therefore recommend the legislative package be reviewed following any amendments to the Privacy Act resulting from the Attorney-General's Department's review.

Recommendation 22: Amend s 154 of the TDI Bill to also require a review of the legislative package to commence no later than 3 months after amendments to the Privacy Act resulting from the Attorney-General's Department's Review of the Privacy Act.

Notifications under digital identity and data breach notifications

59. The legislative package establishes a range of notification obligations for accredited entities and participating relying parties, some of which may arise in the same circumstances as a data breach notification under the Privacy Act. We look forward to further engagement with the DTA on how these obligations can be aligned to promote clarity for regulated entities and reduce notification fatigue for individuals.

60. Where a cybersecurity incident or a digital identity fraud incident occurs, the TDI Bill requires accredited entities and participating relying parties to make all reasonable efforts to contact any individuals affected by the incident and, if applicable, businesses who the affected individual was acting on behalf of.[50] This must occur as soon as practicable after becoming aware of the incident.[51] In addition, accredited entities are required to make all reasonable efforts to keep the individual or businesses informed in relation to the incident, including its management and resolution.[52] The TDI Bill also requires the Oversight Authority to provide reasonable assistance to affected individuals and businesses, including by providing them with contact details of the accredited entities and participating relying parties involved in the incident.[53]

61. Where a cybersecurity incident or a digital identity fraud incident is an eligible data breach as defined under Part IIIC of the Privacy Act, the accredited entity will also be required to notify the individual in accordance with the requirements of the Privacy Act unless it is subject to a comparable State or Territory data breach notification law.[54] An accredited entity subject to a

[49] AGD (Attorney-General's Department), *Review of the Privacy Act 1988*, AGD website, accessed 20 October 2021.

[50] Trusted Digital Identity Bill 2021 (Cth) ss 43-44.

[51] Trusted Digital Identity Bill 2021 (Cth) ss 43-44.

[52] Trusted Digital Identity Bill 2021 (Cth) s 43(6).

[53] Trusted Digital Identity Bill 2021 (Cth) s 46.

[54] Trusted Digital Identity Bill 2021 (Cth) s 68.

comparable State or Territory data breach notification law would presumably be required to notify the individual under the State or Territory law.

62. The OAIC is concerned that the numerous notifications to individuals will lead to notification fatigue such that individuals will no longer treat notifications as serious. We recommend a number of amendments to the current legislative framework to prevent notification fatigue from occurring:

    - The legislation should include a mechanism that means only one accredited entity or participating relying party is required to notify affected individuals or businesses in relation to a particular incident, and should clearly assign the responsibility for notification and engagement with the individual.
    - The DTA should consider how the ongoing obligation on accredited entities to keep affected individuals or businesses informed in relation to the incident can be managed to avoid overwhelming individuals.
    - The threshold for notifying affected individuals and businesses should be carefully considered. Notifications under the NDB scheme are only made to individuals who are likely to experience serious harm as a result of the eligible data breach that has not been prevented through remedial action.[55] This targeted approach avoids causing unnecessary distress to individuals who are not at risk, limits notification fatigue and reduces the administrative cost for regulated entities.

Recommendation 23: The DTA include a mechanism in the legislation that means only one entity is required to notify affected individuals or businesses of a cyber security incident or digital identity fraud incident. This mechanism should clearly assign who has responsibility for notification.

Recommendation 24: The DTA consider the appropriate threshold for when an individual or business will be considered to be 'affected' by a cyber security incident or digital identity fraud incident.

Mandatory consultation

63. Digital identity systems are intricately linked with the collection, use and disclosure of personal information. Given this, any amendments to the legislation, including the Rules, have the potential to create impacts on the privacy of individuals. We note the Minister is required under s 158 of the TDI Bill to conduct a public consultation before making or amending any rules required, permitted, necessary or convenient for the TDI Bill. However, given the role of personal information in digital identity systems we recommend that the Minister should have a specific requirement to consult with the Information Commissioner before making or amending

[55] *Privacy Act 1988* (Cth) s 26WF.

any rules that have an impact on the handling of personal information or the privacy of individuals.

Recommendation 25: Amend the TDI Bill to require the Minister to consult with the Information Commissioner when making or varying rules that have privacy impacts under s 157 of the TDI Bill.