Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D21/18800

27 October 2021

Digital Identity Team
Digital Transformation Agency

By email: digitalidentity@dta.gov.au

Dear Digital Identity Team

Submission in response to Digital Identity Exposure Draft Legislation

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the Digital Transformation Agency's (**DTA**) exposure draft legislation, comprising the:

- *Trusted Digital Identity Bill 2021* (**Bill**);
- *Trusted Digital Identity rules* (**TDI rules**); and
- *Trusted Digital Identity Framework accreditation rules* (**TDIF rules**).

As the primary regulator for information privacy and information security in Victoria, OVIC has a particular interest in the Commonwealth's proposed framework to regulate the Trusted Digital Identity Framework (**TDIF**) accreditation scheme and the Government's Trusted Digital Identity System (**TDIS**).

OVIC is pleased to see several important privacy protections and information security requirements reflected in the Bill and TDIF rules, including additional privacy safeguards when generating or using a digital identity. OVIC supports the DTA's decision to specifically include attributes, restricted attributes and biometric information of an individual in the definition of personal information.[1]

However, in OVIC's view, further work is still required, to ensure it is clear to members of the public:

- what digital identity system is being used to verify or authenticate identity information;
- what the difference is between using the TDIS and other digital identity systems;
- what rights, protections, and safeguards are in place, depending on whether a transaction occurs within the TDIS or under a different digital identity system; and
- what law applies if things go wrong.

This submission comments on broad issues that arise from the complexity of the regulatory framework, as well as specific issues relating to the draft provisions of the Bill, TDI rules and TDIF rules. The submission is focussed on the proposed regulatory and governance model, privacy and consumer safeguards, and

[1] Bill, section 9, definition of 'personal information'.

prohibitions on law enforcement access to digital identity information. For ease of reference, this submission adopts the definitions used in the Bill.

Summary of OVIC's recommendations

Recommendation 1:	Reconsider whether a two-system model of regulation will meet the Bill's objects.
Recommendation 2:	Reconsider whether it is appropriate to make higher levels of regulatory protection dependent on whether a relying party onboards to the TDIS as a participating relying party. In the alternative, the DTA may wish to consider: • applying the same level of regulatory protection whether a relying party is onboarded or not; or • preventing relying parties from transacting with accredited entities.
Recommendation 3:	Reconsider whether it is appropriate to make higher levels of regulatory protection dependent on whether a transaction occurs within the TDIS. In the alternative, the DTA may wish to consider: • applying the same level of regulatory protection to a transaction occurring within the TDIS as a transaction occurring outside the TDIS; or • attaching higher levels of regulatory protection to an onboarded accredited entity, irrespective of whether that entity transacts with an onboarded entity or an entity outside the TDIS.
Recommendation 4:	Reconsider whether trustmarks are appropriate for digital identity.
Recommendation 5:	Consider amending section 7(1) of the TDI rules to insert privacy requirements for a relying party to onboard to the TDIS.
Recommendation 6:	Consider amending section 19 of the Bill to limit the Minister's power to onboard a relying party.
Recommendation 7:	Consider amending section 23(5)(d) of the Bill, to ensure it is mandatory for a PIA to be conducted, and mandatory for the Minister to consider the PIA when deciding whether to make TDI rules specifying kinds of accredited entities authorised to obtain or disclose specified kinds of restricted attributes.
Recommendation 8:	Consider amending the Bill to include an express prohibition on the Minister weighing the matters in section 23(5) in a way that prioritises the expansion of the digital identity market, over the potential harms that could result from the proposed collection or disclosure of restricted attributes, or where the proposed collection or disclosure would be contrary to community expectations.

Recommendation 9:	Consider amending section 74(1) to prevent an accredited entity from sharing restricted attributes with a relying party. Alternatively, consider amending section 74(1) to reflect rule 3.7(2) in Chapter 5 of the TDIF rules, to prohibit an accredited entity from disclosing restricted attributes to a relying party unless the entity is authorised to do so as a condition of the entity's accreditation.
Recommendation 10:	Consider amending section 23(2)(d) of the Bill to make it compulsory for an entity to provide *all* not *any* of the information listed in that section, to ensure *all* information is before the OA when it considers whether to impose a condition on an entity's approval to onboard to the TDIS, authorising the entity to obtain or disclose a restricted attribute of an individual in the TDIS.
Recommendation 11:	Consider amending the Bill to make it mandatory for the TDIF rules to deal with the matters in section 59(2) relating to privacy, fraud and security, compliance and monitoring, and the collection, use and disclosure of attributes, restricted attributes and biometric information of individuals.
Recommendation 12:	Consider amending section 50 of the Bill to elevate the requirement in the TDIF rule to the Bill, requiring applicants undergoing TDIF accreditation to complete a PIA.
Recommendation 13:	Consider amending section 30 of the Bill to make it a requirement to offer an alternative digital and physical channel.
Recommendation 14:	Consider whether the exceptions and exemptions in section 30 of the Bill are consistent with the heading of section 30, and the policy principle underpinning that section, which is that generating and using a digital identity should be voluntary.
Recommendation 15:	Consider amending section 144 of the Bill to insert a prohibition on an accredited entity charging an individual for the creation and use of a digital identity. The prohibition could be modelled off the prohibition on the OA charging an individual in section 140(3) of the Bill.
Recommendation 16:	Consider amending the Bill to include a definition of consent that includes the five elements of consent: voluntary, informed, current, specific, and the individual has the capacity to consent.
Recommendation 17:	Consider amending the TDIF rules to prescribe requirements in relation to obtaining express consent of individuals with respect to biometric information. Consider incorporating into the requirements the five elements of consent, and a direction that consent must be obtained for each new proposed use or disclosure.
Recommendation 18:	Consider whether the exceptions to the prohibition on data profiling in section 80(2) of the Bill, meet the Bill's objects to protect the privacy and

	security of personal information, and to establish a TDIS that is safe and supported by strong privacy and integrity safeguards.
Recommendation 19:	Consider amending section 80 of the Bill to include an express prohibition on the use of personal information to improve the performance or usability of a participant's digital identity system.
Recommendation 20:	Consider amending sections 81(1) and 81(1)(b)(iii) of the Bill, to only permit an enforcement body to access from an accredited entity, digital identity information of an individual for offences relating to identity theft, or the use or misuse of that individual's digital identity.
Recommendation 21:	Reconsider whether sections 81(1)(b)(i) and 81(1)(b)(ii) of the Bill, which permit an accredited entity to provide an enforcement body with access to digital identity information if the enforcement body "reasonably suspects" that a person has committed an offence, is an appropriate threshold for the disclosure of digital identity information to enforcement bodies.
Recommendation 22:	Consider amending section 104(1)(a)(iii) of the Bill, to only permit an enforcement body to access from the OA, digital identity information of an individual for offences relating to identity theft, or the use or misuse of that individual's digital identity.
Recommendation 23:	Consider amending section 61(2) of the Bill to include a mandatory requirement, after receiving a request to deactivate a digital identity, for an accredited identity service provider to ask the individual if they wish to delete their digital identity, and if requested, the accredited identity service provider must delete the digital identity as soon as practicable.
Recommendation 24:	Consider removing the words "or de-identify" from section 132(2) of the Bill, to ensure that accredited entities are obliged to destroy personal information.
Recommendation 25:	Consider amending the TDIF rules to include a requirement that the annual assessment report containing the outcomes of each assessment conducted under the TDIF rules be made available to other onboarded entities in the TDIS, including participating relying parties.
Recommendation 26:	Consider amending section 146(2) of the Bill to insert requirements for the annual report of the OA to include the number of compliance assessments undertaken, the number of failed compliance assessments, the number of suspensions, and the number of revocations.
Recommendation 27:	Ensure the OA and its advisory boards are independent from accredited entities and participating relying parties.
Recommendation 28:	If OA staff are drawn from accredited entities and participating relying parties, consider disclosing this fact publicly, in a timely manner.

Recommendation 29:	Consider replacing the wording in section 158(7) of the Bill with an express statement that a failure to comply with section 158(1) invalidates a rule or amendment to a rule.
Recommendation 30:	Consider amending section 154(2) of the Bill to require a review of the operation of the Act within 3 years of commencement, not two years of commencement.
Recommendation 31:	Consider amending section 154 of the Bill to require regular reviews of the operation of the Act.

OVIC's broad concerns with the regulatory framework

1. OVIC understands the draft legislation creates two voluntary schemes:

    - the TDIF accreditation scheme for providers of identity services (being identity service providers, identity exchanges, attribute service providers, and credential service providers); and

    - the TDIS, which is the Government's digital identity system.

2. Entities can choose to transact inside and outside of the TDIS in the following ways:

    - an entity accredited under the TDIF accreditation scheme (**accredited entity**) can choose to provide its digital identity services outside the TDIS, or onboard to the TDIS (and become an **onboarded accredited entity**), or both. This means an onboarded accredited entity can choose to provide its services inside the TDIS and outside the TDIS; and

    - an entity that consumes or relies on identity services can choose to transact with accredited entities outside the TDIS as a **relying party**, or onboard to the TDIS and become a **participating relying party** (**PRP**)[2], or both. This means it is possible for a relying party to transact with onboarded accredited entities and accredited entities.

3. Under the draft legislation, different levels of regulatory oversight, consumer protections, and liability and enforcement will apply, depending on:

    - whether a relying party is onboarded to the TDIS; and

    - whether a transaction occurs within the TDIS.

4. The following two sections of this submission outline OVIC's concerns about the legislation adopting the above two mechanisms as the trigger for greater regulatory protection. In summary, OVIC is concerned that the mechanisms:

    - are too reliant on relying parties voluntarily onboarding to the TDIS, which is something that individuals and accredited entities have no control over;

    - will result in less regulatory oversight and fewer consumer protections in practice;

    - may lead to trust marks being used by onboarded accredited entities in ways that are misleading; and

[2] Bill, section 9, definition of 'participating relying party'.

- are not easy to understand (particularly in conjunction with the use of trustmarks). Lack of clarity will make it difficult for individuals to make an informed choice to participate in a digital identity system, and to meaningfully choose an identity service provider. Hesitation to generate or use a digital identity will likely have a flow on negative impact on entities who invest time and resources in becoming accredited and/or onboarding to the TDIS, on the false promise that individuals will use a digital identity to obtain or access online services.

Triggering oversight and consumer protections based on whether a relying party is onboarded to the TDIS

5. Under the proposed model, relying parties may operate within or outside of the TDIS. A relying party onboarded to the TDIS as a PRP:

    - will have applied to[3] and met certain requirements to be granted approval to onboard to the TDIS by the Oversight Authority (**OA**)[4] (or the Minister under the TDI rules[5]);

    - will be listed on the TDIS register[6]; and

    - will be permitted to use a trustmark when verifying an identity or attribute through the TDIS.[7]

6. A PRP will also have specific obligations under the Bill and TDI rules, whereas a relying party that is outside the TDIS will not. The specific obligations for PRPs include:

    - the obligation to provide an alternative channel to digital identity, to enable individuals to access the PRP's services;[8]

    - the interoperability principle;[9]

    - complying with conditions imposed by the OA, governing when and how the PRP may use or share attributes,[10] and the services they are approved to provide within the TDIS;[11]

    - meeting extra requirements relating to restricted attributes;[12]

    - notifying individuals, businesses and the OA of any cyber security or fraud incidents,[13] mitigating the adverse effects of cyber security incidents and eliminating or minimising the risk of recurrence of similar cyber security incidents;[14]

    - notifying the OA of other reportable incidents under the TDI rules;[15] and

    - record keeping requirements under the Bill and TDI rules.[16]

[3] Bill, section 16 and Part 6, Chapter 7.
[4] Bill, section 18; TDI rules, section 7.
[5] Bill, section 19.
[6] Bill, section 118.
[7] Bill, section 84(1)(b).
[8] Bill, section 30.
[9] Bill, section 33.
[10] Bill, section 22(6)(b)
[11] Bill, section 22(6)(e)
[12] Bill, sections 22(6)(c), 23 and 74.
[13] Bill, section 44; TDI rules sections 10, 11.
[14] TDI rules, section 18.
[15] TDI rules, sections 12-14, 16.
[16] Bill, section 131; TDI rules, section 19.

7. If a relying party does not onboard and become a PRP it can still transact with onboarded accredited entities. In doing so, the relying party will have saved itself the time and resources involved in applying and meeting the requirements to onboard to the TDIS and complying with the ongoing obligations outlined above. In the circumstances, OVIC queries what incentives there will be for a relying party to onboard to the TDIS.

8. Consequently, if a relying party does not onboard to the TDIS:

    - it will not be required to offer an alternative channel for an individual to access its services, meaning that individuals could be forced to use a digital identity to access or obtain a service from a relying party;

    - it does not have to comply with the interoperability principle, meaning that the relying party could force an individual to use the relying party's preferred identity service provider; and

    - the OA will have no oversight of the relying party's ability to collect and handle digital identity information in a secure and privacy enhancing way.

        - The Information Commissioner will also have no oversight of relying parties that are exempt from complying with the *Privacy Act 1988* (Cth) (**Privacy Act**). This includes small businesses with an annual turnover less than $3M per year, which account for 97.4%-98.4% of all businesses in Australia.[17]

        - Consequently, the regulatory framework enables small businesses to receive attributes and restricted attributes as relying parties, and not be subject to the notifiable data breaches scheme under the Privacy Act or the Australian Privacy Principles when collecting, using or disclosing those attributes and restricted attributes.

        - OVIC is concerned that the lack of regulatory oversight of relying parties could lead to misuse of personal information by relying parties and a corresponding loss of trust and confidence in the use of a digital identity.

9. OVIC questions whether the regulatory framework's heavy reliance on relying parties voluntarily onboarding to the TDIS, undermines the Bill's objects to (1) establish a trusted digital identity system that is safe, secure, trusted, voluntary and supported by strong privacy and integrity safeguards, and (2) to facilitate choice for individuals amongst providers of services within the TDIS.

Triggering liability and enforcement based on whether a transaction occurs within the TDIS

10. The Bill creates different levels of liability and enforcement of the additional privacy safeguards, depending on whether a contravention of the safeguard occurs within the TDIS. It does this by only imposing civil penalties for contraventions that occur within the TDIS,[18] and only granting the Information Commissioner powers of investigation and enforcement for contraventions that occur within the TDIS.[19]

11. OVIC understands that for a contravention to occur *within the TDIS*, *all* participants must be onboarded to the system.[20] Consequently, it appears that civil penalties for breach of the additional

[17] The Australian Small Business and Family Enterprise Ombudsman, *Small Business Counts December 2020*, available at https://www.asbfeo.gov.au/sites/default/files/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2.pdf.
[18] Bill, Chapter 4, Part 2.
[19] Bill, section 119(2)(a).
[20] DTA meeting with Australian Privacy Commissioners, 13 October 2021.

privacy safeguards, and the Information Commissioner's powers of investigation and enforcement of the additional privacy safeguards will not apply to:

- transactions occurring with accredited entities not onboarded to the TDIS; and
- transactions between onboarded accredited entities and relying parties (despite the accredited entity being onboarded).

12. OVIC understands that contraventions of the additional privacy safeguards that occur outside the TDIS will be regulated by the Privacy Act.[21] Under the Privacy Act, the Information Commissioner has power to:

- investigate an act or practice on the Information Commissioner's own initiative or in response to a complaint;[22] and
- enforce[23] a civil penalty for a serious or repeated interference with privacy.[24]

Transactions with accredited entities outside the TDIS

13. In OVIC's view, the enforceable penalties for contravention of the additional privacy safeguards should extend to contraventions by accredited entities operating outside the TDIS. The civil penalty provision in the Privacy Act for a serious or repeated interference with privacy[25] is not an adequate deterrent and does not reflect the sensitivity and value of the personal information travelling within digital identity ecosystems.

14. Enforceable penalties have an important deterrent effect and signal to entities the value of the personal information they are handling, and the seriousness and importance of complying with the privacy safeguards. If one of the objects of the Bill is to ensure that entities participating in other digital identity systems comply with the same strong privacy safeguards as entities operating within the TDIS,[26] it follows that *all* contraventions by accredited entities should be subject to a civil penalty, not just serious or repeated ones.

Transactions between onboarded accredited entities and relying parties

15. OVIC is concerned about a regulatory model that would enable an onboarded accredited entity to evade civil penalties, based only on the fact that the transaction occurs with a relying party who is outside the TDIS. In OVIC's view, onboarded accredited entities should be subject to civil penalties for contraventions of the additional privacy safeguards, irrespective of the status of the relying party.

16. OVIC is also concerned that the use of a TDIS trustmark may be misleading to individuals, given that the civil penalty provisions do not apply if the individual is using a digital identity to obtain or access a service from a relying party. For example, an individual may rely on a TDIS trustmark to choose an identity service provider, on the understanding that this offers greater regulatory protection. However, through no fault of the individual, the services they wish to access are not provided by a PRP. Consequently, the transactions between the onboarded accredited entity and the relying party do not occur within the TDIS, and the greater regulatory protection is not afforded.

[21] DTA meeting with Australian Privacy Commissioners, 13 October 2021.
[22] Privacy Act, section 40.
[23] Privacy Act, section 80U.
[24] Privacy Act, section 13G.
[25] Privacy Act, section 13G.
[26] Bill, section 3(2)(c)(i).

17. The difficulty in explaining to the public how attributes and restricted attributes may travel across entities onboarded to the TDIS and entities not onboarded to the TDIS, and the different regulatory protections that apply to each transaction, means that the 'consent' model suggested as the basis for public engagement with the ecosystem is unlikely to be satisfied.

Trustmarks

18. The proper use of trustmarks is very important to public trust in and the integrity of the TDIS.

19. OVIC continues to be concerned that the creation of different trustmarks and their varying application will be confusing to members of the public, leading to reduced confidence and trust in the use of a digital identity, and in the TDIS. The two-system model will require individuals to understand, in practice, the difference between the trustmarks and the different levels of protection afforded to the individual under each trustmark. Given the perceived confidence that a trustmark imbues, members of the public are unlikely to appreciate that a transaction occurring outside the TDIS offers them less protection and is subject to less regulation than when a transaction occurs within the TDIS.

TDIF trustmark

20. The use of an OA approved TDIF accreditation trustmark exposes the OA to significant reputational risk when an accredited provider is operating outside the TDIS. The OA issued trustmark links the accredited provider's activities back to the OA, and by proxy to the TDIS, irrespective of the fact that the accredited provider was acting outside the TDIS. Consequently, any misuse of personal information by an accredited provider will necessarily impact on public trust in the use of a digital identity and the TDIS.

TDIS trustmark

21. For the reasons outlined at paragraph 16, OVIC is concerned that the use of a TDIS trustmark by an onboarded accredited entity could be misleading, given that greater regulatory protection hinges on a relying party onboarding to the TDIS, rather than an accredited entity onboarding to the TDIS. If, for example, an onboarded accredited identity service provider is permitted to display a TDIS trustmark, how will members of the public understand that different levels of liability[27] and redress obligations[28] will apply, depending on whether the onboarded accredited identity service provider transacts with a relying party or a PRP. The use of a trustmark implies that all transactions operate under the same regulatory protection, which will not be true in practice.

22. Further, if a PRP is permitted to use a TDIS trustmark, it is essential that an ongoing assurance process is in place. At present, the Bill only grants a discretion to the OA to require a PRP to arrange for a compliance assessment to be conducted,[29] and relies on PRP's doing the right thing, by advising the OA of reportable incidents under the TDI rules. OVIC recommends an amendment to the legislation, to require the OA to conduct regular and ongoing reviews of the PRP's compliance with onboarding requirements under the Bill and TDI rules, and any conditions that have been imposed by the OA (similar to the annual assessments for accredited entities under Chapter 7 of the TDIF rules). A TDIS trustmark for a PRP should not be a tick and flick exercise.

[27] See Bill Division 2, Part 2, Chapter 4: Civil penalties for contravention of the additional privacy safeguards only apply if the contravention occurs "within the trusted digital identity system".
[28] See Bill, section 43: the redress framework in Division 3, Part 3, Chapter 2 of the Bill only applies to a service provided by the entity "within the trusted digital identity system".
[29] Bill, section 126(1)(a).

Requirements for onboarding relying parties

Section 18 of the Bill and section 7 of the TDI rules

23. OVIC is pleased to see that relying parties wishing to onboard to the TDIS will need to meet cyber security and fraud incident requirements under section 18 of the Bill and section 7 of the TDI rules. However, there should also be a requirement for a relying party to conduct a privacy impact assessment (**PIA**) or other form of privacy assurance of personal information before onboarding to the TDIS. OVIC strongly recommends an amendment to section 7(1) of the TDI rules, to insert privacy requirements.

24. In OVIC's view, it will be difficult for the OA to set appropriate conditions on the use of attributes and restricted attributes by a PRP, without the knowledge gained from a PIA. Requiring a relying party to turn its mind to how it will collect, use and disclose personal information before onboarding to the TDIS, will help to reduce the risk of a PRP misusing personal information, and damaging the public's trust in the TDIS.

25. If the Bill or TDI rules do not include privacy requirements, participating relying parties may operate within the TDIS, without being subject to any privacy regulation.[30] This is an unacceptable risk to the privacy of digital identity information.

Section 19 of the Bill

26. Section 19 of the Bill grants the Minister power to make TDI rules providing that a relying party is taken to hold an approval under section 18 to onboard to the TDIS.[31] In OVIC's view, this power is too broad.

27. As drafted, section 19 appears to allow the Minister to make rules that would permit relying parties to onboard to the TDIS, without effective oversight by the OA and irrespective of whether they have met the requirements under section 18 and the requirements prescribed in section 7 of the TDI rules. The Bill should not permit this to happen.

28. For individuals to have trust in the TDIS, there must be effective oversight by the OA when a relying party is onboarded to the system. Without oversight, there is no way for an individual to trust that their personal information is not being used and sold by the PRP for the purpose of profiling or other privacy invasive practices. The use of a TDIS trustmark will be problematic if effective oversight of PRP's is not assured through the regulatory framework.

Restricted Attributes

Restricted attributes obtained or disclosed by accredited entities

29. Section 22(8) of the Bill empowers the Minister to make TDI rules specifying kinds of accredited entities authorised to obtain or disclose specified kinds of restricted attributes of individuals, either generally or in specified circumstances. In deciding whether to make the TDI rules, the Minister must have regard to the matters in section 23(5) of the Bill.[32]

30. OVIC recommends an amendment to section 23(5)(d), to ensure it is mandatory for a PIA to be conducted, and mandatory for the Minister to consider the PIA when deciding whether to make the rules.

[30] Businesses with an annual turnover less than $3M are not subject to the Privacy Act.
[31] See Bill, section 19.
[32] Bill, section 23(4).

31. OVIC queries how the Minister will weigh the different matters in section 23(5) to determine which take preference when deciding whether to make the TDI rules under section 22(8). As raised by OVIC during a previous round of consultation,[33] there is an inherent tension between the purposes of creating a safe, secure and trustworthy digital identity ecosystem, and promoting innovation and participation in the digital identity ecosystem. To instil trust in the use of a digital identity, the legislation should make it clear that establishing a trustworthy digital identity system takes precedence over increasing uptake of the system.

32. Consequently, OVIC recommends an express prohibition in the legislation, on the Minister weighing the matters in section 23(5) in a way that prioritises the expansion of the digital identity market,[34] over the potential harms that could result from the proposed collection or disclosure of restricted attributes,[35] or where the proposed collection or disclosure would be contrary to community expectations.[36]

Disclosure of restricted attributes to a relying party

33. The TDIF rules prohibit an accredited entity from disclosing restricted attributes to a relying party unless the entity is authorised to do so as a condition of the entity's accreditation.[37] An exception to this prohibition is disclosure to an attribute verification service.[38] This prohibition is not reflected in the Bill. Instead, section 74(1) of the Bill allows an accredited entity to disclose a restricted attribute of the individual to a relying party (that is outside the TDIS) so long as the accredited entity gains the express consent of the individual.

34. In OVIC's view, accredited entities should be prevented from sharing restricted attributes with relying parties altogether, or at the very least, the TDIF rule should be elevated to the Bill, to ensure that this higher level of protection is legislated.

35. Obtaining the express consent of the individual is not a sufficient safeguard to protect the community from the potential harms that could result from misuse of a restricted attribute. The inadequacy of section 74(1) is particularly stark given:

    - PRP's can only receive restricted attributes if they are authorised by the OA to receive them;[39] and

    - relying parties will not be subject to any regulatory oversight on the use and disclosure of restricted attributes if they are a small business, exempt from the Privacy Act.

36. A system that permits accredited entities to share restricted attributes with relying parties, only on condition that express consent of the individual is obtained, undermines the legislative protections on restricted attributes flowing within the TDIS.

Conditions relating to restricted attributes of individuals

37. Section 23(2) of the Bill sets out matters the OA must have regard to when considering whether to impose a condition on an entity's approval to onboard to the TDIS, authorising the entity to obtain or disclose a restricted attribute of an individual in the TDIS.

---

[33] See OVIC's submission in response to the Digital Identity Legislation Position Paper, 14 July 2021, https://www.digitalidentity.gov.au/sites/default/files/2021-08/22_ovic_0.pdf.
[34] This may be a relevant consideration of the Minister under section 23(5)(e).
[35] Bill, section 23(5)(a).
[36] Bill, section 23(5)(b).
[37] TDIF rules, Chapter 5, rule 3.7(2).
[38] Attribute verification service means a service operated by or on behalf of a Government body which compares personal information in an identity document against Government records: TDIF rules, Chapter 1, rule 1.5(1)(a).
[39] Bill, section 74(2).

38. To ensure the OA has all necessary information before it when considering whether to authorise the entity to receive or disclose a restricted attribute, OVIC recommends an amendment to the Bill to make it compulsory for an entity to provide *all* not *any* of the information listed at section 23(2)(d). This would mean that an entity must provide the OA with a risk assessment plan and a PIA as it relates to the restricted attribute; information on the effectiveness of the entity's protective security, privacy arrangements and fraud control arrangements; and for a PRP, information on the arrangements in place to protect the restricted attribute from further disclosure.[40]

39. OVIC would be deeply concerned if the OA began authorising receipt or disclosure of a restricted attribute without having considered *all* of the information listed in section 23(2)(d).

TDIF rules

40. The Bill lists a number of matters at section 59(2) that the TDIF accreditation rules *may* deal with, not *must* deal with. In OVIC's view the legislation should make it mandatory for the TDIF rules to deal with the matters in section 59(2) relating to privacy, fraud and security,[41] compliance and monitoring,[42] and the collection, use and disclosure of attributes, restricted attributes and biometric information of individuals.[43] These are all matters that go to the heart of a safe, secure and trustworthy digital identity ecosystem. As such, they should not be a discretionary delegation to a legislative instrument that can be subject to change with relative ease and less parliamentary scrutiny than primary legislation.

41. Further, the requirement in the TDIF rules, for applicants undergoing TDIF accreditation to complete a PIA should be enshrined in primary legislation[44], not in the TDIF rules. This would reinforce the importance and value of undertaking a PIA for programs handling high value information and make it harder for this protection to fall away over time.

The use of a digital identity should be voluntary

42. Section 30 of the Bill states that a PRP must not, as a condition of providing a service or access to a service, require an individual to generate or use a digital identity. That is, a PRP must offer an alternative method for an individual to access its service, unless an exception or exemption applies.

43. This is an important protection, to prevent individuals being forced to obtain and use a digital identity, as a precondition to participating in society.

44. However, OVIC is concerned that the protection in section 30 may have little effect in practice:

    - given that it only operates where a transaction is occurring with a PRP and it is entirely voluntary for a relying party to onboard to the TDIS and become a PRP;
    - PRP's and relying parties are not prevented from passing on costs to users; and
    - there is no requirement to provide an alternative *digital* channel as well as an alternative *physical* channel (such as in person or by telephone).

45. OVIC is concerned that in practice a digital identity will not be meaningfully voluntary as:

    - a PRP may choose to offer digital identity as the only digital means of verifying an attribute and may charge for this service, leaving the individual with the choice between paying for

[40] These are the matters listed in section 23(2)(d) of the Bill.
[41] Bill, section 59(2)(a)(i)-(iv) and (b).
[42] Bill, section 59(2)(c)-(d).
[43] Bill, section 59(2)(e)-(g).
[44] OVIC suggests insertion in section 50 of the Bill.

the use of a digital identity or verifying the attribute in person or by telephone, potentially also at cost to the individual; and

- a relying party may require an individual to use and pay for a digital identity as the only means of obtaining or accessing the relying party's service.

46. OVIC is also concerned about the possible negative impacts of the exceptions and exemptions in the Bill, that permit PRPs to force individuals to generate or use a digital identity to access the PRP's service. The exceptions and exemptions must be used sparingly if the use of a digital identity is to be meaningfully voluntary.

Exception for government services

47. The exception in section 30(2)(a) would allow any law of the Commonwealth, a State or a Territory to require verification of the individual's identity solely by means of a digital identity. OVIC suggests the DTA consider whether this exception aligns with the policy principle reflected in the heading to section 30, which is that generating and using a digital identity is voluntary. Individuals should not be forced to generate or use a digital identity to access government services.[45] The Bill should recognise government services as essential and inherently monopolistic, as users cannot choose where and how to access services provided by government.

48. Further, in OVIC's view, government services acting as relying parties, should be required to provide an alternative physical and digital channel to verify identity. An alternative physical channel is particularly important in rural or regional areas, and for those of lower socio-economic status, or who because of health, age or disability may not be able to readily access the technology required to participate in the proposed digital identity system. Government services should be fair, accessible, and equitable for all.

Exemptions from requirement to offer alternative channel

49. Section 30(3) grants a broad power to the OA to grant an exemption to a PRP if the OA "is satisfied that it is appropriate to do so." It will be important for the OA to use this power sparingly, to ensure that as far as is possible, the use of a digital identity is voluntary.

50. Two of the listed circumstances in section 30(4) where the OA may grant an exemption, are where the participating relying party is a small business, or only offers its services online. Online services are a prime use case for digital identity, and small business accounts for between 97.4%-98.4% of all businesses in Australia.[46] In the circumstances, OVIC is concerned that the right of an individual to voluntarily create and use a digital identity will be greatly reduced in practice, if the OA were to grant a high volume of exemptions to small businesses and relying parties that offer services solely online. Innovation and uptake in the TDIS must not come at the expense of an individual's right to participate in society without effectively being forced to obtain and use a digital identity.

Charging by accredited entities

51. OVIC understands the Government's policy position is that it will not impose charges on individuals for the use of a digital identity.[47] This policy position underscores the charging rules, which are intended to be focused on charging arrangements between providers and services using the TDIS, not charges between providers and individuals using a digital identity.[48]

[45] See, among other examples, the answers to questions 10 and 19 at https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/webinar-q-and-a. These answers are not consistent with the exception proposed in the Bill.
[46] The Australian Small Business and Family Enterprise Ombudsman, *Small Business Counts December 2020*, available at https://www.asbfeo.gov.au/sites/default/files/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2.pdf.
[47] Guide, page 44; DTA, Digital Identity Legislation Consultation Position Paper, June 2021, pages 71-72.
[48] Guide, page 44.

52. To ensure the Government's policy is reflected in the Bill, OVIC suggests an amendment to section 144, to prohibit an accredited entity from charging an individual for the creation and use of a digital identity. The prohibition could be modelled off section 140(3) of the Bill, which prohibits the OA from charging a fee to an individual for the creation or use of a digital identity.

Express consent required for the use of biometric information

53. Section 76(1) of the Bill allows an accredited entity to collect, use or disclose biometric information of an individual only if:

    - the collection, use or disclosure is authorised under section 77 or 78 of the Bill; and
    - the individual to whom the information relates has *expressly consented* to the collection, use or disclosure.

54. To be express consent, each of the five elements of meaningful consent needs to be present – that is, it is voluntary, informed, current, specific, and the individual has the capacity to consent. To meet the requirements of being current and specific, consent must be obtained for each new use or disclosure, at the time the new use or disclosure is required.

55. Bundled consents should not be used, whereby an individual is asked to provide consent to the collection, use or disclosure of biometric information for the secondary purpose of testing[49] at the same time as being asked to provide consent for the primary purpose of verifying the identity of the individual or authenticating the individual to their digital identity.[50] To be express consent, the consent for testing should be sought separately, *after* the consent under section 77(1)(c) has been obtained. Further, for the consent to be meaningful, it should be clear that the use of biometric information for testing is optional.

56. OVIC recommends the TDIF rules incorporate the five elements of consent and make it clear that consent must be obtained for each new proposed use or disclosure.[51] OVIC also recommends the Bill include a definition of consent that includes the five elements of consent, to make it clearer to accredited entities that broad consent for multiple purposes is not permitted.

Prohibition on data profiling

57. Section 80(1) of the Bill creates a prohibition on data profiling. Section 80(2) of the Bill then creates exceptions to the prohibition, including:

    - section 80(2)(a), permitting data profiling for the purposes of providing the services for which the entity is accredited;[52] and
    - section 80(2)(b), permitting data profiling if it is for the purposes of the entity complying with the Act.[53]

58. In the previous round of consultation, the DTA's Legislation Consultation Paper stated that one proposed exception was to permit the use of personal information to improve the performance or usability of the participant's digital identity system. It is not clear whether section 80(2)(a) is intended to cover this type of use. The use of personal information for this purpose appears to provide greater benefit to accredited entities, with only minor benefits to a user. Accredited

[49] Bill, section 77(3)(c).
[50] Bill, section 77(1)(c).
[51] The Bill states that the TDIF rules must prescribe requirements in relation to obtaining express consent of individuals to whom the relevant biometric information relates: Bill, section 78(4)(f). However, the TDIF rules do not provide any detail as to the requirements for obtaining express consent.
[52] Bill, section 80(2)(a).
[53] Bill, section 80(2)(b).

entities should be more than capable of improving the performance and usability of their service without using the personal information of users. The proposed use creates significant privacy and security risks for the user, that will almost certainly outweigh any benefits to individual users.

59. OVIC queries whether the exceptions in section 80(2) align with the Bill's objects to protect the privacy and security of personal information and to establish a TDIS that is safe and supported by strong privacy and integrity safeguards. OVIC is concerned that if certain types of profiling are permitted at the outset, scope creep or future additional permitted uses becomes a real and possible outcome over time. This would be detrimental to trust and confidence in the use of a digital identity and the TDIS.

Use of digital identity information for enforcement purposes

Accredited entities

60. Section 81(1) of the Bill allows an accredited entity to use or disclose digital identity information for enforcement related activities conducted by or on behalf of an enforcement body for offences that do not relate to a person's identity. That is, the Bill would allow accredited entities to disclose digital identity information to the police for purposes that bear no connection to identity theft, the digital identity system, or the creation, use or misuse of a digital identity. OVIC is concerned about this broad ability for enforcement bodies to obtain access to digital identity information.

61. Given the sensitive, personal nature of digital identity information, the potential for it to be used across multiple services, and the requisite trust that is needed for an individual to feel safe to use a digital identity, enforcement bodies should only be able to access digital identity information of an individual for offences relating to identity theft, or the use or misuse of that individual's digital identity. Permitting access to digital identity information for a broader range of offences carries a real risk of inadvertently granting surveillance powers to the police. As a free and democratic country, the Government has a duty to protect individuals from being subject to police surveillance.

62. Section 81(1)(b) permits accredited entities to use or disclose information to an enforcement body if at the time the information is used or disclosed, the enforcement body *reasonably suspects* that a person has committed an offence against a law of the Commonwealth or of a State or Territory, or *reasonably suspects* that a person has breached a law imposing a penalty or sanction, or the information is used or disclosed under a warrant.

63. In OVIC's view digital identity information of an individual should only be disclosed under warrant for offences relating to identity theft, or the use or misuse of that individual's digital identity. OVIC is also concerned that it will be difficult, if not impossible, for accredited entities to obtain any further information to satisfy themselves that an enforcement body *reasonably suspects* that a person has committed an offence or breached a law, beyond the word of the police officer who is requesting the information from the accredited entity. OVIC is concerned that this provision could be misused by police, and will lead to scope creep over time.

Oversight Authority

64. Section 104(1)(a)(iii) enables the Oversight Authority to use or disclose protected information if it is done for the purposes of "assisting in the administration or enforcement of another Australian law". OVIC is concerned about this broad power to disclose digital identity information for the enforcement of any other Australian law.

65. OVIC is concerned that section 104(1)(a)(iii) would enable an enforcement body to obtain digital identity information from the OA, in circumstances where the Bill prevents an enforcement body from obtaining the same information from an accredited entity. The threshold for the disclosure of information to enforcement bodies should be the same for the OA as it is for accredited entities.

Deactivation of digital identities

66. The Bill provides that an accredited identity service provider must, if requested to do so by the individual, deactivate the digital identity of the individual as soon as practicable after receiving the request.[54] In OVIC's view, the Bill should be amended to also make it mandatory for an accredited identity service provider to ask the individual if they wish to delete the digital identity, and if requested, the accredited identity service provider must delete the digital identity as soon as practicable.

67. Meaningful consent to the creation and ongoing use of a digital identity needs to be voluntary and current. If no mechanism is provided for the deletion of an individual's digital identity, users who no longer wish to participate in the digital identity ecosystem would be left with a digital identity that they no longer consent to maintaining.

Destruction and de-identification of personal information

68. Section 132(2) of the Bill requires accredited entities to destroy or de-identify personal information held by the entity if, amongst other circumstances, the time period for keeping records under the Bill has elapsed.

69. OVIC is concerned about the ability for accredited entities to retain personal information in de-identified form, particularly where the retention could be indefinite. OVIC recommends the words "or de-identify" be removed from section 132(2), to ensure that accredited entities are obliged to destroy personal information.

70. De-identifying personal information to create aggregate data carries significant risks of re-identification. Permitting de-identification assumes accredited entities will have both the sophisticated technical ability and safeguards in place to prevent re-identification. As has been shown on numerous occasions, de-identification is extremely difficult to achieve, to the point where data remains useful and unable to be reidentified.[55]

71. The Bill does not provide the OA or Information Commissioner with the ability to oversee how de-identified data is utilised by accredited entities, and more concerningly, other private sector entities who may come to possess or otherwise receive this data. OVIC has significant concerns that should this data come into the possession of, for example, entities specialising in analytics or acting as data brokers, the risk of re-identification is high when combined with unrelated data they may already hold.

72. In addition, OVIC is concerned that no legislative restrictions are placed on the proposed uses of de-identified data. In OVIC's view, accredited entities should not be permitted to retain de-identified data for data mining or other commercial purposes. To permit accredited entities to retain data for these purposes will undermine the public's trust in using an accredited entity to generate or use a digital identity.

Effective regulation of the digital identity ecosystem

73. OVIC continues to query the rationale for creating two different regulatory systems for the OA to oversee and enforce: regulation of accredited entities and regulation of onboarded accredited entities and PRPs.

[54] Bill, section 61(2).
[55] See, Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) data release - https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records and Release of Victorian public transport (Myki) data - https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf.

74. OVIC is concerned about the ability of the OA to regulate two separate schemes. In addition to the work involved in approving and auditing onboarded accredited entities, the OA will need to be significantly resourced to:

    - effectively audit accredited entities who participate in digital identity systems that the OA does not regulate or have direct oversight. If the OA is not properly resourced to audit accredited entities, OVIC foresees situations where accredited entities are not TDIF compliant, exposing personal information to risk of misuse and damaging the public's trust in using a digital identity; and

    - effectively onboard and audit PRPs in the TDIS. If the OA is not properly resourced to have effective oversight of PRPs, OVIC foresees situations where PRPs are not compliant with the Bill and TDI rules, exposing personal information to risk of misuse and damaging the public's trust in the TDIS.

75. OVIC is also concerned about the ability of the Office of the Australian Information Commissioner (**OAIC**) to take on additional functions and powers under the Bill and offer meaningful regulatory protection for contraventions that occur outside the TDIS. The OAIC's funding and resource constraints in relation to its existing and numerous important functions and responsibilities has been well-publicised. For the additional privacy safeguards to be effective, the OAIC will require significantly more staff and resources to enable it to respond to privacy complaints in a timely manner, and effectively utilise the Information Commissioner's own initiative investigation powers under the Privacy Act, and the new powers of investigation and enforcement in the Bill. If the OAIC is not properly funded and resourced, the OAIC will not be able to offer meaningful redress to individuals affected by a contravention of the additional privacy safeguards and the civil penalty provisions will remain unenforced.

Transparency mechanisms

76. OVIC is pleased to see the types of information proposed to be listed in the TDIF and TDI registers.[56] The registers are an important transparency mechanism, essential to building trust in the digital identity ecosystem. To further enhance transparency, and trust for entities to invest in accreditation and onboard to the TDIS, OVIC recommends that:

    - the annual assessment report[57] containing the outcomes of each assessment conducted under the TDIF rules be made available to other onboarded entities in the TDIS, including PRPs; and

    - section 146(2) of the Bill is amended to ensure that the annual report of the OA includes the number of compliance assessments undertaken, the number of failed compliance assessments, the number of suspensions, and the number of revocations.

Location of the OA

77. OVIC understands that the Government is still considering which Government entity will house or support the OA.[58] OVIC reiterates the importance of housing the OA in a place that enables it to operate with sufficient independence to exercise its statutory duties effectively.

78. To avoid any moral hazard, the OA will need to be completely independent from accredited entities and PRPs. This means that the OA and the advisory boards should be staffed with individuals who do not have a vested interest in furthering the uptake of the TDIS.

[56] Bill, sections 117 and 118.
[57] Prepared in accordance with Chapter 7, Part 2, Rule 2.5(1) of the TDIF rules.
[58] DTA, Your guide to the Digital Identity legislation, page 8.

79. If staff are drawn from accredited entities and PRPs, the OA should be transparent about this with entities in the ecosystem and the wider public.

Minister's requirement to consult before making or amending any rules

80. Given the substantial number of matters of substantive policy that are left to the TDI rules and TDIF rules, it is pleasing to see a requirement to consult in section 158 of the Bill. OVIC would like to see this provision strengthened by replacing section 158(7) with an express statement that a failure to comply with section 158(1) invalidates a rule or amendment to a rule.

Review period

81. Section 154(2) requires the Bill to be reviewed no later than 2 years after its commencement. In OVIC's view, this review period is too short to gain a considered view of how the legislation is operating in practice. Given the length of time it will take to set up the OA, accredit entities and onboard entities to the TDIS, OVIC considers the review should be undertaken no less than 3 years after the Act's commencement.

82. OVIC also recommends an amendment to section 154 of the Bill, to require regular reviews of the operation of the Act. Ongoing reviews will be important, to ensure the Act continues to meet its objects into the future.[59]

Thank you again for the opportunity to comment on the DTA's draft 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.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Emma Stephens, Senior Policy Officer, at Emma.Stephens@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner

[59] Bill, section 3.