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: D21/11953

14 July 2021

Digital Identity Team
Digital Transformation Agency

By email: digitalidentity@dta.gov.au

Dear Digital Identity Team

**Submission in response to the Digital Identity Legislation Position Paper**

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the Digital Transformation Agency's (**DTA**) Digital Identity Legislation Position Paper (**position paper**).

As the primary regulator for information privacy, information security and freedom of information in Victoria, OVIC is particularly interested in proposed developments to the Commonwealth's Digital Identity system (**DI system**) and Trusted Digital Identity Framework accreditation scheme (**TDIF accreditation scheme**). OVIC welcomes the opportunity to provide further input into the development of Trusted Digital Identity Legislation (**Legislation**). In doing so, OVIC's aim is to ensure that the Legislation establishes permanent privacy protections, and strong governance structures for the DI system and TDIF accreditation scheme. In OVIC's view, this is necessary to build community trust in the DI system. Without such trust, the DI system is unlikely to be successful.

For an individual to have trust and confidence when using a digital identity to obtain a service from government or private enterprises, it must be clear to the individual:

- who the participants in the digital identity system are;
- whether the digital identity or attribute is being generated or shared within the DI system or outside of the DI system;
- what rights, protections and safeguards are in place, depending on whether the transaction occurs within the DI system or outside of the DI system; and
- who to complain to if things go wrong.

For the reasons set out in this submission, OVIC's view is that the above matters are not made clear in the position paper, and that further work is required before members of the public can have the requisite confidence and trust to use a digital identity.

This submission also provides general comments on the proposed governance of the DI system, as well as specific comments on the proposed privacy and consumer safeguards, drawing on themes that OVIC has

previously raised with the DTA in earlier consultations on the proposed digital identity legislation. For ease of reference, this submission adopts the definition of terms used in the position paper.

**Primary purpose of the Legislation should be clear**

1. OVIC is concerned that the inherent tension between the purposes of creating a safe, secure and trustworthy DI system, and promoting innovation and participation in the DI system, needs to be, but is not currently, addressed in the position paper or the proposed Legislation.

2. With respect to trust in the DI system, the position paper states that "One of the key purposes of the Legislation is to ensure privacy and consumer safeguards within the TDIF are enshrined in law, providing enhanced protections for User data and personal information on the system…. By enshrining privacy and consumer safeguards in law, the Legislation will instil greater trust in the system as it is rolled out to more services".[1] The position paper also states that "The TDIF accreditation scheme and the Digital Identity system are designed to provide Users, TDIF Providers, Accredited Participants and Participants alike, a safe and secure framework to access and provide digital identity services".[2]

3. With respect to innovation, the position paper notes that previous feedback highlighted differences between the views of private sector entities and government stakeholders, and that private sector entities were concerned that "the Legislation may put pressure on entities to choose between digital identity systems, limiting opportunities for innovation."[3] The DTA appears to have given weight to this feedback from private sector entities, as the position paper states that one of the three key principles guiding the development of the privacy and consumer safeguard policies is "fostering participation and innovation". This is described as "the need for strong consumer and privacy protections has been balanced against the requirement to foster participation in the system, and to enable technological and other forms of innovation as the system grows".[4]

4. The position paper appears to adopt the view that the two legislative purposes (trust and innovation) are of equal value and can co-exist in harmony. However, there will be circumstances where they conflict (for example, in providing regulatory backing for the trust between identity providers (**IDPs**), attribute service providers, and relying parties, versus facilitating growth in the digital identity economy), and a choice will need to be made as to which purpose takes precedence. The Legislation should make that choice, by clearing stating its *primary* purpose.

5. OVIC is concerned that failing to clearly articulate that the primary purpose of the Legislation is to create a safe, secure and trustworthy DI system, could lead to many technical changes over time (which the position paper notes are not disallowable), which prioritise participation and innovation, over important privacy safeguards that instil trust in the DI system.

**Proposal to separate regulation of the TDIF Accreditation Scheme from regulation of the DI system**

6. OVIC understands from the position paper that the proposed Legislation will serve two purposes:

    - Regulating TDIF accreditation, to allow an identity provider (**IDP**), identity exchange, attribute service provider and credential service provider to be TDIF accredited, irrespective of whether they

[1] Position paper, section 3.5, page 9.
[2] Position paper, section 3.5.1, page 10.
[3] Position paper, section 5.2, page 14.
[4] Position Paper, section 7.1, page 44.

participate in the DI system. If they do not participate in the system they are referred to as 'TDIF Providers' and if they do participate in the DI system, these entities are referred to as 'Accredited Participants'.

- Regulating the operation of the DI system and Accredited Participants within the DI system.

7. The position paper proposes that TDIF Providers will be subject to the same privacy safeguards as Accredited Participants (which OVIC queries further below) and will be subject to reporting to the Oversight Authority (**OA**). However, TDIF Providers will not be subject to civil penalties or the redress framework that Accredited Participants will be subject to under the Legislation. While speculative, OVIC is concerned entities may strategically choose to remain a TDIF Provider to avoid being subject to civil penalties and the redress framework. This would be an undesirable outcome, to the detriment of users.

8. OVIC queries the rationale for creating two different regulatory systems for the OA to oversee and enforce: regulation of TDIF Providers and regulation of Accredited Participants in the DI system.

9. OVIC is concerned about the ability of the OA to regulate two separate schemes. The OA will need to be significantly resourced to effectively audit TDIF Providers 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 TDIF Providers, OVIC foresees situations where TDIF Providers are not TDIF compliant, exposing personal information to risk of misuse.

**Privacy and consumer safeguards, penalties and enforcement of TDIF providers**

10. OVIC queries whether the position paper is misleading in its assertion that TDIF Providers operating outside the DI system will be subject to the same privacy and consumer safeguards as Accredited Participants operating in the DI system.[5] OVIC is concerned that this statement is misleading for two reasons:

    - Section 7 of the position paper, which deals with privacy and consumer safeguards, does not mention TDIF Providers at all. Instead, the position paper proposes for the legislative privacy and consumer safeguards to apply to Accredited Participants in the DI system.

    - The position paper states that TDIF Providers will not be subject to the same civil penalties, redress scheme, or enforcement under the Legislation (except for misuse of a trustmark).

11. In OVIC's view, this is a significant weakening of privacy and consumer safeguards when using a TDIF Provider. Unlike an Accredited Participant in the DI system, the TDIF Provider will not be subject to enforcement of privacy safeguards by the Office of the Australian Information Commissioner (**OAIC**) and monitoring and enforcement of compliance with the Legislation by the OA.

12. Further clarification is needed as to whether TDIF Providers will at least be subject to the privacy and consumer safeguards in section 7 of the position paper. For example, the proposed legislative safeguards on biometric information, restrictions on data profiling, prohibition on the use of a single identifier and requirement of express consent, appear to only apply to the DI system, not to TDIF Providers using other digital identity systems. Further, the legislative requirement for IDP's, attribute service providers, credential service providers and identity exchanges to be subject to the

[5] Position Paper, sections 3.3 and 3.4, page 8.

Commonwealth Privacy Act or a comparable state or territory privacy law, appears to only apply to Accredited Participants in the DI system, not TDIF Providers. OVIC considers that it should be a legislative requirement for TDIF Providers to be subject to privacy laws, and to the extra protections proposed under the TDIF irrespective of whether they operate within or outside the DI system.

13. The requirement to notify the OA of a data breach also only appears to apply to Accredited Participants in the DI system, not TDIF Providers. OVIC considers that it would be difficult for the OA to audit a TDIF provider's ongoing accreditation if there is no legislative requirement for the TDIF Provider to report data breaches to the OA.

14. It should be clear to members of the public exactly what protections will be in place when they choose a TDIF Provider that is not using the DI system, and how these protections differ from the protections in place if they choose an Accredited Participant who uses the DI system. Without this clarity, users cannot have confidence and trust in the use of a digital identity, either within or outside the DI system.

**Regulating TDIF accreditation**

15. The position paper proposes that TDIF Providers will be subject to OA reporting and that the Legislation will provide an enforceable set of rules[6] for TDIF Providers based on the standards currently in place.[7]

16. In contrast, Accredited Participants in the DI system will be subject to legislative penalties and enforcement, and administrative sanctions by the OA for breaching the Legislation or a TDIF accreditation rule, and administrative sanctions by the OAIC for breaches of key privacy safeguards.

17. OVIC queries how the OA will effectively regulate a TDIF Provider who is not on the DI system, if it cannot utilise the same legislative powers that are proposed for regulating Accredited Participants.

18. OVIC also queries what transparency mechanisms will be in place to inform users of a TDIF Providers compliance with TDIF rules. It will be important for TDIF Providers to be regularly audited, given that they are permitted to operate in digital identity systems that are not regulated by the OA. There should be a commitment to make these audit reports public.

19. Further, the proposed requirement for applicants undergoing TDIF accreditation to complete a Privacy Impact Assessment (**PIA**) should be enshrined in primary legislation, not in the rules. This would reinforce the importance and value of undertaking a PIA for programs handling high value information, and will assist applicants to identify risks and implement mitigation strategies.

20. PIAs should not be viewed as a compliance exercise, or an exercise that is required to unduly burden the resources of parties wanting to be TDIF accredited. To minimise the perceived impact of undertaking a PIA, the DTA or OA (in consultation with the OAIC or other regulators) could develop a set of PIA templates or other materials that provide targeted guidance to each type of participant in the system.

[6] OVIC notes that instruments such as rules can be subject to change with relative ease and less scrutiny than primary legislation.
[7] Position Paper, section 3.3, page 8.

**Multiple digital identity systems and the use of trustmarks**

21. The position paper proposes the use of one or more trust marks; one for TDIF accreditation, and one for a TDIF accredited entity who is participating in the DI system as an Accredited Participant.[8]

22. Under the proposed model, OVIC understands that it will be possible for Accredited Participants in the DI system to transact with entities outside of the DI System. Figure 6 on page 27 of the position paper indicates that it will be possible for an IDP that is an Accredited Participant, to create a digital identity for a user and share that digital identity through an identity exchange that is outside the DI system, to a relying party that is also outside the DI system. In this scenario, the only participant in the DI system is the IDP. The position paper suggests that in this scenario, the IDP is acting as an Accredited Participant in the DI system. Figure 7, on page 28, also shows an interaction where an attribute service provider shares an attribute directly with an outside relying party, with no intermediary identity exchange. Once again, the position paper states that the attribute service provider is acting as an Accredited Participant in this scenario.

23. OVIC is concerned about a model that operates in this way. The proper use of trustmarks in these scenarios is very important to public trust in and the integrity of the DI system. In the Figure 6 scenario, which trustmark will the IDP be permitted to display? If the IDP is permitted to display the trustmark that indicates the entity is using the DI system, OVIC considers this to be misleading and confusing to users, as there will be no way for a user to know that the identity exchange has occurred outside of the DI system, and that the identity exchange is therefore not subject to civil penalties for non-compliance, or subject to the redress framework in circumstances where there has been an inappropriate disclosure of information, identity theft, cyber security incident or system failure.

24. A related issue is how and where the trustmark will be displayed. If it is permitted to be displayed on a relying party's website, to indicate that the user can use a digital identity to access the relying party's service, this will likely be misleading to members of the public, who may understandably, but incorrectly, attribute the trust and confidence inherent in a trustmark to the relying party. This issue is particularly stark in circumstances where the relying party is a small business, and therefore not subject to the requirements in the Commonwealth Privacy Act. In this circumstance, the user has relied on the trustmark, but has no ability to seek recourse for a misuse of their personal information by the small business relying party.

25. Further, OVIC is concerned that the creation of different trustmarks and their varying application to Accredited Participants and TDIF Providers will be confusing to members of the public, leading to reduced confidence and trust in the use of a digital identity and the DI system. 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 using a TDIF Provider offers them less protection than using an Accredited Participant.

26. Lastly, the use of an OA approved TDIF accreditation trustmark exposes the OA to significant reputational risk where a TDIF Provider is operating outside the DI system. The OA issued trustmark links the TDIF Provider's activities back to the OA, and by proxy to the DI system, irrespective of the fact that the TDIF Provider was acting outside the DI system. Consequently, any misuse of personal

[8] Position Paper, section 8, page 57.

information by a TDIF Provider will necessarily impact on public trust in the use of a digital identity and the DI system.

27. The model appears to fail to fulfil one of its stated purposes to "provide clarity for Users".[9] Explaining to the public the circumstances in which one trustmark has a different level of protection to the other is a very serious hurdle for this model to overcome.

28. To ensure public trust, it must be clear which parties are subject to the DI system for each transaction that takes place, and therefore which regulatory regime and consumer and privacy safeguards apply to each transaction. This will be difficult to achieve under the proposed model.

**Relying parties operating in and/or outside of the DI system**

29. Under the proposed model, relying parties may be in or outside of the DI system. If they are inside the DI system they will have applied to and been granted access to the DI system by the OA, will be listed on the Participant Register, and will be permitted to use a trustmark when verifying an identity through the DI system.

30. A relying party that is in the DI system will also have specific obligations under the Legislation, whereas a relying party that is outside the DI system will not. The specific obligations for relying parties in the DI system include:[10]

    - the interoperability principle;
    - complying with conditions governing when and how they may use or share attributes;
    - meeting extra requirements relating to restricted attributes;
    - notifying the OA of any security or fraud incidents impacting the system and assisting with resolution; and
    - the obligation to provide an alternative channel to Digital Identity to enable individuals to access its services, subject to various proposed exceptions discussed later in this submission.

31. OVIC is concerned that under this model, there may be little incentive for relying parties to be in the DI system. Relying parties not being in the DI system leads to a corresponding loss of the safeguards identified above, and a loss of public trust and confidence in the use of a digital identity and the DI system.

32. OVIC also queries how the protections on restricted attributes will operate in circumstances where a relying party that is not in the DI system requests the restricted attributes from an attribute service provider within the DI system. In OVIC's view attribute service providers and IDP's within the DI system should be prevented from sharing restricted attributes with relying parties that are not in the DI system. If they are free to share restricted attributes, this greatly waters down the proposed legislative protections on restricted attributes, as the protections will only work if a relying party decides to participate in the DI system, which is something that the user has no control over. In OVIC's view, the

[9] Position Paper, section 3.5, page 9.
[10] Position Paper, section 5.4.14, page 30.

proposed model does not provide adequate protection to the community from the potential harms that could result from a restricted attribute being disclosed to an unauthorised third party.

33. The difficulty in explaining to the public how these various attributes may travel across entities in the DI system means that the 'consent' model suggested as the basis for public engagement with the ecosystem is unlikely to be satisfied.

**Privacy safeguards for relying parties in the DI system**

34. The position paper proposes that relying parties in the DI system will not be subject to the same additional privacy safeguards as Accredited Participants in the DI system. Instead, relying parties will remain subject to any privacy law that applies to them in providing their services.

35. OVIC's view is that relying parties in the DI system should be required to undergo a PIA and be subject to privacy law. A requirement to be subject to privacy laws, or to at least undergo a PIA, is particularly important in circumstances where relying parties may not otherwise be subject to any privacy law at all, such as small businesses, who are currently exempt from complying with the Commonwealth Privacy Act.

36. As previously noted, PIAs should not be viewed as a compliance exercise, or an exercise that is required to unduly burden the resources of parties wanting to participate in the DI system. PIAs enable parties to identify risks, and implement strategies to mitigate those risks. Noting the more limited role – from a technical and operational perspective – that Relying Parties play in the DI system, undertaking a PIA would not be an onerous task – even where resources are limited (for example NGOs and small businesses).

37. If a requirement to undertake a PIA were included, to minimise the perceived impact, the OA could develop a set of templates or other materials that provide targeted guidance to relying parties.

38. At a minimum, the OA should be satisfied that the exchange of digital identity information to a relying party (and any subsidiaries) will be unlikely to result in a privacy or security breach.

**Choice and alternative channels**

39. The position paper notes that creation and use of a digital identity will be voluntary for individuals, with a requirement for relying parties to have an alternative channel for accessing their service, unless an exemption applies. The position paper also notes that this principle was supported in submissions to the consultation paper.

*Essential and monopolistic services*

40. OVIC queries whether there is a typographical error at 7.4.1 of the position paper. The sentence reads:

    *"It is also proposed the Bill will require a relying party using the system to provide an alternative channel to Digital Identity to enable individuals to access its services **provided** the relying party's service is **not** an essential service (such as a welfare benefit) or is the only provider of that service (i.e., a monopolistic service)" (**emphasis added**).*

41. The sentence suggests that essential services and monopolistic services do not need to provide an alternative channel to access their service. In OVIC's view it is critical that essential and monopolistic

services are required to provide an alternative channel, given that by their very nature, users have no choice but to use the service. It would be anathema to the principle that a digital identity is voluntary if essential and monopolistic services were permitted to force individuals to use a digital identity. A system cannot be voluntary in situations where coercion exists. It cannot be considered voluntary if it is impossible to apply for an essential government service without a digital identity.[11]

42. The position paper also states that an exemption will be provided for an essential or monopolistic service that is legislatively required to provide a particular service or activity through digital means only. The position paper gives the example of legislation requiring reporting to the Australian Taxation Office (**ATO**) by large businesses to be done digitally. OVIC opposes this proposal. For the reasons stated, there should be no exemptions allowed for essential and monopolistic services.

43. OVIC encourages the DTA to consider all government services as essential and inherently monopolistic, as users cannot choose where and how to access services provided by government. Further, in OVIC's view, government services acting as relying parties, should be required to provide an alternative *physical* channel to verify identity, not just an alternative digital channel, as proposed in the position paper. This 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 for small business and online services*

44. Other proposed circumstances in the position paper for granting an exemption to the requirement to offer an alternative channel, are where the relying party is a small business, or the entity 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.[12] In the circumstances, OVIC queries the policy rationale behind these exemptions, given that they will greatly reduce, in practice, an individual's right to voluntarily create and use a digital identity. OVIC is concerned that priority is being given to innovation and uptake in the DI system, at the expense of an individual's right to participate in society without effectively being forced to obtain and use a digital identity.

45. Furthermore, no use cases have been presented where proof of identity may be necessary to obtain services provided by small businesses, and it is difficult to understand what purpose this exemption may fulfil. While small businesses may be interested in obtaining attributes to fulfil a transaction, this can be achieved without the burden of identity proofing. In practice, many modern browsers and operating systems already provide this functionality, so the provision of such a service to small businesses would appear to be a solved problem, albeit without the involvement of an identity federation.

**Risk of commercialisation of identity and on passing costs to users**

46. The position paper sets out a proposed charging framework under the Legislation guided by seven charging principles.[13] Principle 3 of the proposed charging principles in the Legislation, states that the

[11] See, among other examples, the answers to questions10 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 exemptions proposed in the position paper.
[12] 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.
[13] Position Paper, section 11.4.2, page 73.

Australian Government will not charge users for the creation or use of a Digital Identity. Principle 3 then states that users may be charged by relying parties, as it is open to relying parties to pass on the costs.

47. OVIC is concerned that allowing relying parties to pass on the cost to users will result in the DI system being commercialised from a consumer perspective and that a digital identity will not, in fact, be free. This is particularly concerning in situations where the relying party is permitted to not offer any alternative channel to receive their service.

48. OVIC cautions the DTA against a model that relies on commercialising the DI system or seeks to create a market in digital identity. Examples of international digital identity systems that have utilised cost recovery or for-profit models, such as GOV.UK Verify, demonstrate that creating a market for, and involving multiple identity providers comes at a risk of consumer confusion and low uptake, and ultimately identity providers withdrawing from the system.[14] OVIC highlights that out of the seven identity providers that signed up for the GOV.UK Verify program only two remain.

49. The key policy drivers for the DI system should be to provide secure, efficient, and economical access to government and private sector services and transactions, and a reduction in identity fraud and identity theft. These policy outcomes will be impacted if the commercial success of the DI system is prioritised.

50. OVIC notes that there may be good reasons for involving the private sector in an identity federation, but any such considerations should be done on the basis of equitable access, privacy, and the integrity of the identity ecosystem. Commercial considerations should always be secondary to these three objectives.

**Transacting anonymously**

51. When utilising the services of a relying party, OVIC queries whether individuals will be able to verify their attributes in a way that is not personally identifying. OVIC recommends that safeguards be put in place to ensure that relying parties only request the minimum attributes necessary to receive the service, and that permit individuals to transact anonymously with relying parties in circumstances where it is not necessary to be identified to receive the service. This could be achieved through technical specifications and requirements that build in privacy by default.

52. If data minimisation is not enabled by default and anonymous transactions are not possible, this raises a significant risk of over-collection of personal information. This concern is heightened where a relying party is not subject to privacy laws (for example, a small business) and is exempt from the requirement to provide an alternative means of obtaining the service, as the individual will have no choice but to accept the over-collection of their personal information.

53. Further, where it is not necessary for a relying party to receive the attribute in order to provide the service to the individual, OVIC recommends that the relying party only receive an indication that the attribute has been successfully verified, rather than receiving the attribute itself (for example, if the person needs to be over 18 to access a service, the system could display to the relying party a green tick when age is verified, instead of displaying the person's age or age range).

[14] The UK National Audit Office's investigation into the GOV.UK Verify program highlighted the inconvenience to users and the cost implications to both the public and private sector when commercial identity providers enter an identity system and then subsequently withdraw. See https://www.nao.org.uk/report/investigation-into-verify/.

54. Entities currently collecting personal information to satisfy other regulatory requirements (for example, nightclubs, where proof of age is required, and mobile telephone SIM card sellers, which require validation of identity for anti-money laundering and counter terrorism finance protection), are examples of current weaknesses in protection against identity theft and fraud, where consideration should be given to limit data collection, rather than enhancing it. The DTA has said it will collaborate with AUSTRAC to develop systems to assist know your customer (**KYC**) requirements.[15] This work should be aimed at reducing the need for KYC to collect attributes, where identity can be assured by an IDP.

**Biometric information**

55. The position paper states that the Legislation will allow for random sampling of biometric information that has not yet been deleted to test and refine matching algorithms, and to inform anonymous aggregate reporting on biometric accuracy.[16] The position paper states that this is subject to the testing being done after obtaining user consent and states that this consent can be obtained either when the user provides the biometric information or prior to the testing occurring.

56. Consent should only be obtained prior to the testing occurring. Consent to random sampling of biometric information should not be bundled with consent to providing biometric information for the purposes of identity verification to use a service. For consent to be meaningful it must be current, specific and voluntary. Bundling consent, as proposed in the position paper, does not meet these requirements.

**Restrictions on data profiling**

57. The position paper proposes that the Legislation will prohibit Accredited Participants from collecting, using and disclosing information about a user's behaviour on the system. The paper then lists several exceptions to the prohibition on data profiling.[17]

58. In OVIC's view, the purpose of the DI system is to provide individuals with access to a privacy enhanced federated digital identity system. This is not achieved where profiling is permitted. In addition, 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 DI system.

*Improve performance or usability of the participant's digital identity system*

59. One exception is to permit the use of personal information to improve performance or usability of the participant's digital identity system. OVIC does not support the use of personal information for this purpose. This proposed use of personal information appears to provide greater benefit to IDP's and attribute service providers, with only minor benefits to a user. Participants in the DI system 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.

[15] See the Answer to question 6 at: https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/webinar-q-and-a.
[16] Position Paper, section 7.4.2, page 46.
[17] Position Paper, section 7.4.3, page 48.

*De-identify the data to create aggregate data*

60. OVIC is also concerned with the proposed exception of permitting user information to be de-identified to create aggregate data due to the significant risk of re-identification. Permitting de-identification to occur assumes Accredited Participants 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.[18]

61. It appears the DTA may not have fully considered the scenarios and contexts in which de-identified aggregate data may be used both inside and outside the DI system. Neither the OA or OAIC will have the ability to oversee how de-identified aggregate data is utilised by participants, and more concerningly, 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 data analytics, the risk of re-identification is high when combined with unrelated data they may already hold.

62. In addition, OVIC is concerned that no legislative restrictions are placed on the proposed uses of the aggregate data (beyond the overarching prohibited purposes listed on page 49 of the position paper). In OVIC's view, the purposes for using aggregate data should be limited to uses that are in the public interest, and these purposes should be clearly spelt out in primary legislation.

**Requirement of express consent**

63. It is proposed that the Legislation will require a user to expressly consent before an Accredited Participant authenticates and sends attributes to a relying party. When developing the mechanism for this consent, the DTA should ensure each element of meaningful consent is considered – that is, it is voluntary, informed, current, specific, and the individual has the capacity to consent.

64. The position paper states that the requirement for a user to expressly consent before an Accredited Participant authenticates and sends attributes to a relying party "will accommodate a user's ability to provide enduring consent to an identity exchange for attributes to be passed if the user returns to the same relying party (for example, a user could tick a box saying 'do not display next time')".[19]

65. OVIC is concerned that the DTA's reference to enduring consent indicates that the DTA has not considered all elements of meaningful consent. By its nature enduring consent will not be current or specific. It is also not clear how enduring consent can be given in a double-blind system where the IDP or attribute service provider will not know who the relying party is. OVIC recommends that the DTA further consider how express consent will operate in practice under the DI system.

**Application of privacy laws**

66. The position paper notes that state and territory government entities will have the option of complying with a comparable state or territory privacy law, instead of needing to comply with the Commonwealth Privacy Act.[20] Whilst this is a welcome development, OVIC recommends that the Legislation be drafted in a way that makes it clear that where a state or territory government entity does have a comparable

[18] 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.
[19] Position Paper, section 7.4.6, page 51.
[20] Position Paper, section 7.4.14, page 55.

state or territory privacy law, that law *will apply*, rather than granting the state or territory the *option* to comply instead with the Commonwealth Privacy Act.

67. In OVIC's view, it is not preferable to allow state parties with comparable privacy laws to opt-in to federal privacy laws, as this will cause confusion as to the jurisdiction of the relevant privacy regulator. Further, measures to ensure the continuity of individuals' privacy rights and ability to make privacy enquiries and complaints should be assured. It should be clear to individuals who the relevant party is (for example, the OA or relevant privacy regulator) to receive privacy enquires and complaints.

68. For states and territories without comparable privacy laws, OVIC queries whether the proposed mechanisms in the position paper will provide the OAIC with sufficient jurisdiction to enforce federal privacy laws against a state or territory entity. It is OVIC's experience that binding entities or instrumentalities to privacy obligations (either under legislation or via contract) does not necessarily allow for the enforceability of those obligations across jurisdictions.

69. OVIC also reiterates concerns raised during a previous consultation with Privacy Commissioners[21] regarding the potential for the proposed digital identity reforms to intersect with human rights, as well as the Commonwealth Government's eSafety agenda. OVIC recommends the DTA consider the cumulative impact the overlapping nature of digital reforms may have on individuals' right to privacy – particularly when transacting with government.

**Overlapping regulation of privacy compliance and privacy laws**

70. Under the proposed regulatory system, the OA and the OAIC appear to have concurrent oversight roles. OVIC has concerns about the OA (and not the OAIC) assessing an organisation's compliance with privacy laws for TDIF accreditation and onboarding to the system. The question as to whether an applicant is compliant or not with privacy laws should rest with the OAIC. For example, the OA may accredit a participant and the OAIC subsequently take a different view as to their privacy compliance, as part of regulating the additional privacy protections under the system.

71. In relation to the proposed information sharing powers between regulators, to manage data breaches under the system effectively, OVIC would be glad to work with other privacy regulators to establish necessary operational information sharing processes.

**Governance of the DI system**

72. While it is positive that the regulatory functions of the OA will be separated from policy and rule-making functions, 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.

73. To avoid any moral hazard, the OA will need to be completely independent from TDIF Providers, Accredited Participants and relying parties in the DI system. 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 DI system.

[21] On 23 February 2021.

74. Additionally, for the OA to effectively govern the TDIF accreditation scheme and DI system, OA staff will need to have specialist skills and training in audit and/or investigation, as well as expertise in IT, to fulfill accreditation functions and ensure that the operation of the various entities is within the scope of the scheme. Of the example agencies identified in the position paper [22]as potentially providers of resources to the OA, only the ATO and Australian Competition and Consumer Commission might be expected to have staff trained in investigations or audits. Further, the ATO may be conflicted in providing any staff (and especially IT staff) as it is possible the ATO, as an IDP or as a relying party, might need to be the subject of regulatory action (this conflict may also apply to other agencies that act as providers or relying parties, for example, Services Australia). Furthermore, a secondment model will make it less likely the OA will develop any of this expertise itself, over time. OVIC suggests the model requires considerable further scrutiny in order for the independence of the OA to be assured, including in relation to resourcing decisions.

75. To ensure that there is effective governance and oversight, the OA should be well-resourced to conduct audits and own-motion investigations. If a particularly powerful participant in the DI system is non-compliant and does not rectify deficiencies, the OA needs to have sufficient power and resources to enforce rectification outside any political or participant interference. Further, as stated earlier in this submission, the OA will need to be sufficiently resourced to conduct regular and effective audits of TDIF Providers' compliance with the TDIF accreditation scheme.

*Transparency mechanisms*

76. OVIC recommends that clear and comprehensive reporting and audit mechanisms be included in primary legislation. The nature of a federated identity scheme requires that all participants have trust that other entities in the scheme are abiding by the Legislation and rules. To that end, OVIC recommends the Legislation require the publication of reports and audits required under the system.

77. Transparency mechanisms, such as reporting obligations and audit requirements, also serve as an important, albeit indirect, protection for individuals' privacy. Comprehensive transparency mechanisms may expose failed audits, providing individuals with important information to make better choices about their personal information.

**Offboarding from the system**

78. If an IDP leaves the DI system, there should be clear obligations for the destruction, deletion, retention or transfer of digital identity information, in line with relevant privacy, information security or record-keeping obligations. The potential for individuals' digital identity information to be retained by a former provider no longer part of the system poses unacceptable privacy and security risks.

79. If an IDP has been offboarded from the DI system, the position paper states, on page 42, that it will be relatively simple for a user to establish a digital identity with another provider as "Meta-data and logs of a user's previous Digital Identity may be linked to their current Digital Identity through a system-run process that is designed to identify a Digital Identity of the same individual." OVIC cautions against this process being used in circumstances where the IDP was offboarded due to its inability to meet accreditation requirements or requirements to participate in the DI system, such as requirements as to quality and accuracy of information, or where the IDP has been used for fraud.

[22] Position Paper, section 6.4.3, page 35.

**Deletions and end-of-life handling of digital identities**

80. OVIC notes that there is no proposal to allow a user to delete their digital identity. Instead, there will be record keeping requirements to retain the digital identity for 7 years. Meaningful consent to the creation and ongoing use of a digital identity needs to be voluntary and current. To ensure this threshold is met, it will be necessary to include a mechanism in the proposed Legislation to enable users to opt-out of the DI system after they have created a digital identity. This mechanism should also allow for the deletion of a user's digital identity. Without such a mechanism, users who no longer wish to participate in the DI system would be left with a digital identity that they no longer consent to maintaining.

**Overlapping nature of identity reforms**

81. OVIC queries whether the DTA has done any work to assess how the safeguards for biometric information will interact with other proposed reforms across government, such as the *Identity-matching Services Bill 2019* (**IMS Bill**).[23]

82. OVIC reiterates the point made during previous consultation[24] noting the potential legislative scope creep between the proposed Legislation and other, overlapping schemes, such as the scheme proposed under the IMS Bill, including the proposed Face Verification Service (FVS).

83. While OVIC recognises that it is not the intention for the proposed Legislation to extend to the FVS, the nature of scope creep is inadvertent. If the IMS Bill does progress (as well as future proposed digital identity reforms), it will become important to ensure that overlapping digital identity reforms do not inadvertently weaken protections under the DI system. OVIC suggests the DTA map how the proposed digital identity reforms may interact with relevant reforms in other portfolios, to avoid future for legislation scope creep, such as in the current telecommunications environment.[25]

Thank you again for the opportunity to comment on the position paper. 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**

[23] The Parliamentary Joint Committee on Intelligence and Security's Advisory Report on the Bill includes recommendations relating to biometrics and privacy, from [5.7] onwards.
[24] OVIC's response to the DTA dated 2 March 2021.
[25] For example, the interaction of powers to intercept communications between the *Telecommunications (Interception and Access) Act 1979* and the cumulative amendments made to the *Telecommunications Act* 1997, such as those under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (relating to encrypted communications).