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: D20/22605

18 December 2020

Digital Identity Team
Digital Transformation Agency

By email only: digitalidentity@dta.gov.au

Dear Digital Identity Team

Submission in response to the *Digital Identity Legislation* consultation 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* consultation paper (**the paper**).

As the primary regulator for information privacy, information security, and freedom of information in Victoria, OVIC has a particular interest in the developments to the Commonwealth's digital identity system (**DI system**) and the Trusted Digital Identity Framework (**TDIF**). OVIC welcomes the opportunity to provide input into the development of a legislative framework establishing permanent privacy protections and governance structures for the DI system.

This submission is organised around certain questions posed in the paper, and draws on themes that OVIC has previously raised with the DTA in earlier consultations on the proposed digital identity legislation.

Question 1A: Are the matters above (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation?

Each of the matters raised – authority for the expansion, maintenance and regulation of the DI system, embedding privacy protections, establishing permanent governance arrangements, and making consequential amendments – should be included in the proposed legislation.

Including these matters in the legislation will ensure the DI system operates efficiently and predictably in its transition from operating under a policy framework to that of a legislative framework. Additionally, the inclusion of statutory privacy protections and permanent governance arrangements in the proposed legislation will be crucial to ensuring both users' and accredited participants' trust in the DI system.

Question 2A: What matters covered by the TDIF should be incorporated into the primary legislation?

As OVIC has previously raised with the DTA,[1] there are significant privacy, security and operational risks associated with maintaining the TDIF as a 'policy document' that could be subject to change or modification with little transparency or meaningful consultation with stakeholders. As the system expands, undue political or commercial pressure could result in modifications to the TDIF, weakening protections and technical elements to the detriment of the public who use the system.

As the system is expanded beyond Commonwealth Government organisations and becomes available to states, territories, and private sector organisations, these new organisations would better appreciate the

[1] In OVIC's response to the DTA's Digital Identity Legislation scoping paper.

serious, sensitive and valuable nature of services they will be offering if the TDIF is wholly subsumed into the proposed legislation and legislative instrument/s.

Noting the above views, in respect of the proposed legislation, OVIC considers that the existing protections and prohibitions contained in *TDIF 04: Functional Requirements* must be incorporated into the proposed legislation. Many of these elements – privacy protections, fraud control, and protective security requirements – will be critical to achieving public buy-in and trust in the DI system. Public confidence in the system would be boosted with the knowledge that organisations are legislatively bound to operate in a particular way, with appropriate privacy and security mechanisms in place.

In addition, OVIC notes that paragraph 3.2.1 of the paper contains a number of items that are proposed to be included in the Operating Rules, as opposed to the primary legislation. OVIC considers that the items concerning the enforcement powers of the Oversight Authority (the power to terminate or suspend participants, issue infringement notices, and seek civil or criminal penalties) and compulsion powers of the Oversight Authority (direct or compel information from participants to undertake inquiries or investigations) must necessarily be included in the proposed legislation.

Enforcement and compulsion powers are typically contained in legislation, as opposed to legislative instruments, as they should not be subject to modification without parliamentary scrutiny. Given the significance of the use of these powers by the Oversight Authority – for example terminating a participant's involvement – it is crucial that the processes and procedures for their use, as well appeal mechanisms are set out in detail and contained in the primary legislation.

Question 5: Are the concepts outlined above appropriate to include in a definition of 'Digital Identity' for the Legislation? Are there any additional concepts that should be included?

Paragraph 3.3.3 of the paper notes the legislation will define 'Digital Identity', setting out what a digital identity is, who can have a digital identity, what it can be used for and any limitations on its use. The concepts outlined in the paper are appropriate for inclusion in the definition of 'Digital Identity'.

In addition, OVIC suggests that the definition of 'Digital Identity' sets out that a digital identity is free (that is, at no cost) to use and access by consumers, and that creating a digital identity is voluntary. Including these additional concepts in a primary definition will assist to ensure the DI system isn't commercialised from a consumer perspective at later date, and convey to the public up front that a digital identity is voluntary.

Question 6: Does the Legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

In OVIC's view, it would be preferable for the proposed digital identity legislation to leverage the definitions of personal information, sensitive information and protected information as contained in existing Commonwealth Acts, by referring to the relevant definitions contained in other legislation. Including a new definition for 'digital identity information' that duplicates elements of the existing definitions will cause unnecessary confusion and regulatory uncertainty, particularly if those definitions in other legislation change in the future.

This is particularly so for 'personal information' used in the DI system, which has an existing definition[2] and established regulatory framework under the *Privacy Act 1988* (Cth) (**Privacy Act**). Referencing existing definitions will also ensure existing rights, obligations or protections under the relevant Act or Acts will continue to apply in the context of the DI system.

[2] See section 6 of the Privacy Act.

Noting this and as raised in Appendix 2 of the paper, the current review of the Privacy Act should be monitored by the DTA to understand how future reforms may impact on the operation or regulation of the DI system.

Question 7: What factors should be considered in the development of a charging framework for the system?

OVIC cautions the DTA against a model that relies on commercialising the DI system or seeks to create a market for digital identity. Examples of international digital identity systems that have utilised cost recovery models, such as GOV.UK Verify,[3] demonstrate that creating a market for, and involving multiple identity providers comes at a risk of consumer confusion and low uptake. 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.[4] It is notable that out of the seven identity providers that signed up for the GOV.UK Verify program, five no longer allow new identities to be created using their systems, and each of those providers will withdraw from the system completely on 24 March 2021.[5]

The key policy drivers for the DI system should be to provide efficient and economical access to government and private sector services and transactions, and a reduction in fraud and identity theft. These policy outcomes may be impacted if commercialising the DI system and seeking to involve multiple identity providers is prioritised.

Question 9A: Should the proposed privacy and consumer protections listed above be enshrined in primary legislation?

As noted in response to question 2A, including privacy protections and restrictions on the use of personal information will be critical to achieving public buy-in and trust in the DI system. Public confidence in the system will be enhanced with the knowledge that DI system participants are legislatively bound to comply with strict privacy and consumer protections.

OVIC is of the view that each of the privacy and consumer protections outlined in paragraph 4.2 of the paper should be included in the proposed legislation. In particular, OVIC emphasises the importance of ensuring the creation of a digital identity is voluntary, and all transactions and processing of personal information within the system are done with the user's consent.

Additionally, OVIC highlights that the requirement to not create or use a unique identifier across the DI system is critical. Stakeholders and the public remain particularly concerned that the system could be repurposed, or over time, and with scope creep, become an equivalent to the 'Australia Card'. Embedding this particular element in legislation will assist to dissuade those concerns and demonstrate that the DI system is not intended as a national identity credential.

Question 11A: What types of profiling of behavioural information should be prohibited and allowed?

The existing restrictions contained in the TDIF should be replicated in the proposed legislation. This should also extend to prohibiting the use or collection of service history information. Permitting the use of this information provides only minor benefits to a consumer and creates significant privacy and security risks for the individual. Permitting any level of profiling or use of service history information appears to provide greater benefit to Identity and Attribute Service Providers – such as marketing and targeted advertising.

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, or service use history is made available to

[3] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.
[4] https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf at page 24.
[5] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

parties involved. In addition, if certain types of profiling are permitted, or not prohibited at the outset, scope creep or future additional permitted uses becomes a real and possible outcome over time. This would be detrimental to the public's trust and confidence in the DI system.

Question 14A: Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

A requirement for the user to provide their consent before transacting with a relying party should be included in the legislation. This will enable users to understand what attributes will be disclosed or collected by the relying party, and provide users with greater control to choose which attributes are shared. 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.[6]

Question 14B: Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt out of the system after they have created a Digital Identity?

As noted in our response to question 14A, meaningful consent 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 consented to maintaining.

Question 17: Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

OVIC suggests that the requirement for participants to undertake a Privacy Impact Assessment (**PIA**) as part of the accreditation process be recognised in the proposed legislation. This would reinforce the importance and value of undertaking a PIA for programs handling high value information, and will assist participants to identify risks and implement mitigation strategies.

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 program. To minimise the perceived impact of undertaking a PIA, the DTA or Oversight Authority (in consultation with the Office of the Australian Information Commissioner (**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.

Question 22B: What is the optimal structure of the new body?

The paper outlines three options for the Oversight Authority. These include functions being performed by:

- an existing Commonwealth entity or company;
- a new Commonwealth entity or company;
- a new Corporations Act company (limited by guarantee or shares).

In OVIC's view the optimal model is either a new or existing independent Oversight Authority with a statutory appointee. This model will ensure the requisite independence to provide effective and appropriate regulatory oversight of both Commonwealth and private sector participants.

Any other proposed option contains within it an element of moral hazard: if the Oversight Authority is a Commonwealth entity, for example the developer of the TDIF, there is a vested interest in the success of the ecosystem. Likewise, if the Oversight Authority is a company or commercial entity, there is a vested

[6] See discussion of the elements of consent in OVIC's *Guidelines to the Information Privacy Principles* for further information: https://ovic.vic.gov.au/book/key-concepts/#Consent.

interest in ensuring the commercial viability of the ecosystem, which as previously noted in this submission, is not a favourable approach in OVIC's view. In each in of these examples, the Oversight Authority's vested interest in the DI system could result in them minimising potential breaches or non-compliance to avoid a loss of trust in the DI system or otherwise minimise financial or economic impacts to their operations.

Furthermore, as has been the case in other government accreditation programs, if a particularly powerful participant in the federation is non-compliant and does not rectify deficiencies, an Oversight Authority that does not have statutory independence may be politically powerless to enforce rectification.

Question 23: What type (or types) of information should be required to be publicly reported by the Oversight Authority, to increase transparency in the system?

In addition to the matters detailed in paragraph 5.2 of the paper, OVIC is of the view that an effective federation requires that participant audit reports be made available to all federation relying parties. Without this information, relying parties (which may include state or territory government agencies) cannot adequately assure themselves of the risks inherent in relying on participants who may be non-complaint with the proposed legislation, operating rules, or TDIF.

Question 31: Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?

The proposed approaches set out in paragraphs 6.3.1, 6.3.2 and 6.3.1 of the paper appear to be an appropriate approach to achieving a high degree of consistency in relation to privacy protections. The approaches detailed will ensure that all participants in the DI system are subject to some form of privacy legislation.

As noted in paragraph 6.3.2 of the paper, OVIC would value the opportunity to engage with the DTA to determine how 'equivalency' of privacy protections can be achieved, and the how the *Privacy and Data Protection Act 2014* (Vic) will operate in the context of Victorian Government organisations operating in the DI system.

Thank you for the opportunity to consult and provide comment on the development of the digital identity legislation. I have no objection to this submission being published by the DTA 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 the DTA 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 Cliff Bertram, Principal Policy Officer at cliff.bertram@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner