Privacy Commissioner
Te Mana Mātāpono Matatapu

Submission on Digital Identity Services Trust Framework Rules

Introduction

1. Thank you for this opportunity to submit on the Digital Identity Services Trust Framework Rules.

2. Under the Privacy Act 2020, the functions of the Privacy Commissioner include examining new legislation for possible impacts on individual privacy. It is also part of my role to monitor emerging privacy issues, and to offer guidance on how people in industry, government agencies, and across broader society can uphold their privacy obligations.

3. My office has engaged on and supported the Digital Identity Services Trust Framework ("the framework") throughout its development. My interest is to ensure the framework:

    - Will protect New Zealanders' privacy and uphold trust;
    - Will be consistent with and support the role of my office under the Privacy Act.

Upholding privacy is critical for digital identity services to succeed

4. I welcome the continued approach of proactively considering privacy in the development of the framework. Upholding privacy will be critical for digital identity services to succeed. With that in mind, some key points from my perspective are:

    - **Digital identity services involve, collecting, sharing, and using personal information**, and these activities are subject to Privacy Act requirements.
    - **The Privacy Act remains the starting point for responsible handling of personal information**. The legal framework for digital identity services adds to and does not override existing Privacy Act requirements.[1]
    - **All aspects of the digital identity framework are subject to the Privacy Act**. The Privacy Act does not only require steps to uphold privacy and confidentiality, but also sets out obligations around how information is collected and used, ensuring accuracy, and providing access to information. These obligations are relevant across all of the five identified categories for proposed rules.

5. My key recommendation is to make it clearer that the Privacy Act applies across the full scope of the rules, to avoid a mistaken impression that it is limited to the "privacy" category established under the proposed rules. See further analysis below.

---

[1] Section 17 of the Digital Identity Services Trust Framework Act 2023 ("DISTF Act") provides "[n]othing in this Act overrides the Privacy Act 2020".

It should be clearer that the Privacy Act applies across all rules categories

6. The proposal presents Privacy and Confidentiality as one category of rules. However, it is important that everyone reading the rules will have a clear understanding that Privacy Act requirements apply across the whole framework and each rules category.

7. The Privacy Act's Information Privacy Principles set out legal requirements for:

- Collection of personal information (IPPs 1-4)
- Use of personal information, including security requirements (IPP5) and limiting use of personal information based on the purpose it was collected for (IPP10)
- Access and correction of personal information (IPPs 6-7)
- Ensuring personal information is accurate (IPP8)
- Retention of personal information (IPP9)
- Disclosure of personal information (IPPS 11-12)

8. Specific Privacy Act requirements will be critical for particular rules categories as below.

Rules category	Description	Key privacy issues
Identification Management	Rules for determining the accuracy of personal or organisational information, binding that information to an individual or organisation, and enabling the secure reuse of the bound information.	Accuracy Collection from the subject Use
Sharing and Facilitation	Rules for facilitating the sharing of information with relying parties including authorisation (consent) requirements.	Use, Disclosure, Purpose
Privacy and Confidentiality	Rules for trust framework providers to ensure the privacy and confidentiality of the information of individuals or organisations to whom the information relates is maintained.	Use, Disclosure, Security
Security and Risk	Rules ensuring information is secure and protected from unauthorised modification, use, or loss.	Security
Information and Data management	Rules for managing personal and organisational data to ensure a common understanding of what is shared.	Accuracy Access

9. I recommend that the Rules document clearly explain how the Privacy Act applies. This explanation could appear in the Overview and draw on the points at [4] above.

Comments on the proposed Rules

Identification Management Rules

10. We support the proposed rules overall, and particularly requirements that:

    - Users MUST be able to request revocation of a credential issued to them, and this must occur as soon as practicable (IM5.5).

    - Subjects MUST be able to request revocation of a credential containing their personal information (IM5.6).

11. We view these requirements as supporting Privacy Act requirements relating to access and collection of personal information.

Sharing and Facilitation Rules

12. We have no particular comments on this aspect of the Rules.

Authorisation Rules

13. We support requirements to limit the scope of authorisation, and view these as giving effect to Privacy Act requirements which limit the use and sharing of information based on the purpose for which it was collected.

Privacy and Confidentiality Rules

14. We welcome the clear explanation that "[t]he Trust Framework Privacy Rules supplement the requirements under the Privacy Act and do not replace any existing obligations". As above, we would like to see a similar statement for the Rules as a whole.

15. We support clear requirements to comply with the Privacy Act and its Information Privacy Principles, including requirements to:

    - Produce a privacy impact assessment (at PV1.3) and review it at least every two years (PV1.4)

    - Limit use of information collected for the purpose of a digital identity service transaction or obtain explicit consent (PV1.13)

16. We also welcome the requirement for privacy training, including on privacy complaints processes. We encourage continued communication with our Investigations and Dispute Resolution team to ensure complaints handling and transfers are efficient and practical.

Security and Risk Management Rules

17. Overall we support the listed requirements. We recommend the following changes:

    - At SR1.13, following the requirement to report significant cyber incidents to the Trust Framework Authority, we recommend adding "…and must also satisfy breach reporting requirements under the Privacy Act 2020."

18. In addition to the requirements already listed, you may wish to include:

    - **Implementing the principle of least privilege to mitigate risk from overly broad access credentials**.[2] This is related to but distinct from the risks of weak human resource security (DIS.R01), credential loss (DIS.R04), insecure API endpoints (DIS.R05), weak access controls (DIS.R09), and unauthorised use of credentials (DIS.R11). In the event that there is unauthorised access for any of these reasons, credentials with a narrower scope of access (eg fewer permissions, fewer users, shorter durations) will mitigate privacy and security risk.

Information and Data Management Rules

19. We support requirements to have solid information and data governance practices in place, and to review them every two years. We also support requirements to:

    - Consider Māori cultural perspectives (IF2.1) and inform users where information is stored and processed (IF2.2).

    - Include details to support investigations or analysis of compliance (IF3.1).

    - Retain information for a retention period set by regulations (IF3.2). In our submission on the regulations we identified that setting this retention period is a key policy decision, which needs to strike a balance between data minimisation while supporting principles of information access and accountability.

20. Both the NCSC Cyber Security Framework and the Institute of Directors' "Cyber risk a practical guide (2023) refer to privacy as a governance issue and may be useful resources to refer to in this context.

Glossary

21. We welcome the reference to s 7(1) of the Privacy Act 2020 as the definition for personal information.

---

[2] See eg CERTNZ "Principle of least privilege", <cert.govt.nz>.

22. The glossary also sets out the following text in black. We propose the addition in blue and with underlining.

Term	Description
Privacy requirements	Ensuring the privacy and confidentiality of the information of individuals or organisations is maintained. These requirements are in addition to Privacy Act requirements which must also be satisfied.

Conclusion

23. Thank you again for the opportunity to make this submission.

Ngā mihi nui,

Michael Webster

Privacy Commissioner