2 June 2026

Digital Identity Consultation
Digital and Identity Policy Team
Department of Internal Affairs
By email: DigitalIdentity.Consultation@dia.govt.nz

Tēnā koutou

Discussion document: Privacy and security of digital identity information held by the Department of Internal Affairs

The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the invitation to provide feedback on the above consultation. The following response has been prepared with assistance from the Law Society's Human Rights and Privacy Committee, following the template provided in your discussion document.

Questions for feedback

Part One: Collection

1. Under a decentralised model such as the Trust Framework, should the Department consider having its own additional safeguards as to when information is able to be collected (especially given that it could be later used by third parties)?

The Law Society considers that, in a decentralised digital identity environment, reliance on the Privacy Act 2020 alone may not be sufficient. Additional safeguards should be adopted at the point of collection to reflect the increased risks associated with downstream use by third parties. These should include:

a) Collection should be strictly limited to what is necessary for clearly defined and lawful purposes, expressly linked to credentialisation use cases.

b) There should be a strong presumption against speculative or anticipatory collection of identity information for potential future credentialisation purposes.

c) The Department should ensure meaningful transparency, including clear notification that collected information may be used to generate credentials that are subsequently relied upon by third parties.

d) Consideration should be given to requiring that information collected is, where feasible, capable of being transformed into privacy-enhancing derived attributes, in order to minimise subsequent disclosure risks.

2. What do you consider is the Department's responsibility in protecting identity information once it sits within a decentralised ecosystem?

The Law Society considers that the Department's responsibilities do not end once information enters a decentralised ecosystem. The Department remains a system steward and risk originator. It retains an ongoing obligation to ensure that the system it designs and operates maintains public trust. This includes establishing enforceable baseline standards for downstream use, implementing technical controls that support privacy by design, and enabling effective audit and oversight. Its responsibilities should extend to:

a) setting baseline rules for downstream handling of any credential derived from its data;

b) ensuring technical enforceability of privacy controls (not just contractual terms);

c) maintaining trust assurance, including audit capability and revocation mechanisms; and

d) ensuring that ecosystem design aligns with Privacy Act principles, particularly IPPs 1–4 and 10–11, even where third parties operate independently.

3. Should the Department be able to create derived information from information that it has collected from customers?

The creation of derived information is, in principle, a positive development that can enhance privacy by reducing the need to disclose underlying identity attributes (e.g. age verification rather than date of birth disclosure). However, such derivation should be subject to clear limitations, including ensuring that derived attributes do not enable re-identification or functionally reconstruct the underlying data when combined, such as:

a) derivation should be limited to defined, legitimate purposes;

b) derived attributes must be designed to avoid re-identification risk; and

c) there should be restrictions on combining derived attributes that could create underlying identity data.

4. Are there other future models for collecting digital identity information you can identify that could better preserve privacy and security for identity information held by the Department?

The Law Society notes that alternative models may offer more robust long-term protection of identity information and should be actively explored, such as:

- Attribute based collection (collect only what is necessary to generate credentials, not full identity datasets).
- User-mediated verification at source (data remains with authoritative source, not copied).
- Zero-knowledge proofs or cryptographic attestations, in appropriate use cases (i.e. ways to prove something is true without revealing the underlying personal information).
- Event based collection rather than persistent storage.

Part Two: Storage

5. Is storage of Department handled information something you see as appropriate for third parties to be able to do in a decentralised digital environment?
    a. If so, what are the minimum 'must have' controls/evidence that should be required before the Department allows a third party to handle/consume a Department created credential?
    b. Given that the Trust Framework does not deal with relying parties, are there additional safeguards and requirements the Department should consider for the information that it holds on behalf of New Zealanders?

The Law Society considers that the storage of Department-held identity information by third parties should not be the default position in a decentralised environment. Rather, it should be permitted only where there is a clear and justifiable need, such as compliance with statutory obligations (e.g. AML/CFT requirements).

Permitting third party storage should be exceptional, use-case driven, and tightly controlled – not default.

In general, access-based verification should be preferred over third party storage, as this better aligns with data minimisation principles and reduces systemic risk.

Where third party storage or handling is permitted, the following minimum controls should apply:

- demonstrated compliance with the Privacy Act 2020, including cross-border disclosure requirements;
- accreditation under the Trust Framework (or equivalent assurance mechanisms), particularly for higher-risk use cases;
- independent security assurance (e.g. recognised certification);
- strict data minimisation and retention obligations;
- robust audit, monitoring, and incident reporting requirements; and
- acceptance of enforceable contractual obligations, including regulatory oversight.

6. If so, are there additional protections that could be considered to ensure that storage is safe (e.g., should Department created credentials work exclusively with Trust Framework accredited services)?

Yes, particularly for relying parties which are not directly regulated by the Trust Framework. Recommended additional protections include:

a) mandatory baseline obligations imposed by the Department as issuer;

b) standard form data handling conditions embedded in credential use; and

c) a tiered trust model based on sensitivity of information.

The Law Society supports restricting certain credentials, particularly those involving higher-risk or more sensitive attributes, to use within accredited environments.

7. What visibility should the Department require (e.g., storage locations, incident reporting) to maintain safe storage in a decentralised ecosystem? Do these need to go above and beyond the controls in place under the Trust Framework or the Privacy Act?

    a. Should the Department require that any subcontractors/downstream parties handling Department credential data meet the same conditions as the primary provider? What visibility should the Department require across the supply chain?

The Department should require location of storage (including offshore transfers), breach/incident reporting (aligned with Privacy Act notification requirements), audit logs and assurance reporting, and periodic independent certification. These should go beyond baseline Privacy Act compliance, given the scale of systemic risk.

Regarding subcontractors / the supply chain – yes, flow down obligations must apply contractually and technically. The Department should require full supply chain

transparency, equivalent security/privacy obligations, and the ability to audit or require assurance reporting.

8. If you do not consider it appropriate for third parties to store information the Department holds on behalf of New Zealanders, is there a way for the Department to be able to completely prevent third parties from being able to store any information that is important to the Department?
    a. Would this be possible to achieve under the Trust Framework?
    b. If not, what are other, effective ways to prevent our information from being stored by third parties, through technological or other means?

It is not realistic to expect that storage by third parties can be completely prevented once information is disclosed. This reflects both the practical realities of how digital systems operate and the limits of regulatory and contractual enforcement.

The Trust Framework, in its current form, is unlikely to fully achieve this outcome, particularly given that it does not regulate all relying parties.

However, the risk of downstream storage can be materially reduced through a combination of:

- credential design (including selective disclosure and time-limited attributes);
- technical controls that discourage or prevent copying;
- legal and contractual restrictions; and
- a general preference for access-based verification models.

Accordingly, the focus should be on risk minimisation rather than absolute prevention.

9. Are there additional considerations around how we can (or should) restrict third parties from storing our information?
    a. Should the default be 'access-based verification',[1] rather than third party storage or bulk transfer?
    b. How should AISAs or APIs be treated under the new system? Would we do anything differently?

[1] Access-based verification is type of verification where the third party doesn't receive or keep its own copy of the personal information; instead the third party logs into a controlled environment where the data already lives (e.g. an agency system, approved platform) and does what they need there.

The Law Society considers that access-based verification should be the default model, with any departure from this model requiring clear justification.

Additional considerations include:

a) whether storage introduces disproportionate security risk relative to the benefit;

b) whether the same outcome could be achieved through non-retention models; and

c) whether the proposed storage is consistent with IPP9.

AISAs/APIs should be retained as important tools, but progressively reoriented towards real-time, access-based verification, rather than bulk data transfer. In particular, the Law Society considers that:

- bulk transfer models should be used sparingly and justified;
- APIs should incorporate data minimisation and purpose limitation by design; and
- existing AISAs may require review to ensure alignment with decentralised identity principles.

10. How can we consider data sovereignty in an appropriate manner in a decentralised system? Are there requirements or conditions we should consider for third parties if they are storing information the Department handles?

    a. Would third parties need to, for example, store Department held information specifically in New Zealand based servers?

Data sovereignty considerations should be addressed explicitly. At a minimum, there should be a strong preference for storage in New Zealand or at least in jurisdictions with comparable privacy protections, consistent with IPP12.

11. Should there be additional safeguards as to when the Department can and cannot store information?

Yes – internal safeguards should also tighten clear retention limits tied to purpose, and avoid unnecessary centralisation duplication in a decentralised model.

12. Are there other future models for storing digital identity information that you can identify that could better preserve privacy and security for digital identity information held by the Department?

- Distributed storage with user control (wallet-based).
- Federation identity verification models, where multiple trusted parties participate in verifying identity information under a shared framework, rather than relying on a single central authority.
- No persistent storage for certain high-risk attributes.

Part Three: Use

13. What are the minimum 'must have' controls/evidence that should be required before the Department allows a third party – including a relying party – to handle/consume a Department issued credential presented by a user?

The Law Society considers that the Department should impose minimum assurance requirements before permitting any third party to rely on or consume Department-issued credentials. These should include:

a) accreditation or equivalent assurance threshold;

b) purpose limitation and use restrictions;

c) appropriate security and technical controls ensuring use does not become storage;

d) user consent clarity at point of presentation;

e) defined liability and accountability framework.

14. Should the Department consider some level of visibility (e.g., usage logs, incident reporting) to maintain confidence in the use of identity information in a decentralised ecosystem?

In the Law Society's view, some degree of system-level visibility will be appropriate to maintain trust in the overall ecosystem, including incident reporting and audit capability. These should be proportionate and privacy-preserving, and care must be taken to avoid creating mechanisms that amount to centralised tracking of individuals' use of credentials (as that presents a trust risk).

15. Are there additional protections that should be considered to ensure that credential use is legitimate (e.g., should the Department created credentials work exclusively with Trust Framework accredited services)?

a. If we allow third parties to use the information that the Department holds on behalf of New Zealanders, are there additional requirements or conditions that we should consider on top of what is set out under the DISTF Act so that we are satisfied they will handle information appropriately? If so, what could those be?

b. Should access to sensitive credential attributes require demonstrated capability (training/certification) for both agency and third-party personnel? If yes, what should be mandatory?

Access to more sensitive credential attributes should require demonstrated capability, which may include mandatory training or certification of relevant personnel.

Additional protection should be considered, such as:

- Sensitive credentials should be restricted to accredited services.
- Contextual integrity rules should be implemented (i.e. use only in expected context).
- Attribute-level access controls.

The Law Society agrees that there should be additional requirements beyond the DISTF Act, such as:

- enforceable issuer-imposed conditions of use;
- liability allocation for misuse; and
- enhanced audit and enforcement powers.

For sensitive attributes, privacy and security training should be mandatory. Certification tiers should be aligned to data sensitivity.

16. If a third party fails to meet expectations (assurance, incident response, retention), what consequences should apply (e.g., suspension, revocation, limitation to low sensitivity attributes) and who triggers them?

The Law Society supports a graduated enforcement framework for non-compliance, ranging from warnings through to suspension or revocation of access, with escalation for serious breaches. The triggering party would be the Department and/or Trust Framework Authority.

17. Are there risks that arise where the Department uses information from other government agencies or third parties? If so, what safeguards should there be as to when the Department can use that information? What considerations do you see being in play?

The Law Society agrees that risks arise where the Department relies on information sourced from other agencies or third parties (function creep and issues with data integrity). In such cases, the Department should ensure that use is clearly authorised, consistent with the original purpose of collection, and subject to appropriate quality assurances.

18. Are there other future models for using digital identity information you can identify that could better preserve privacy and security for the identity information held by the Department?

- Techniques that enable information to be verified or analysed without disclosing the underlying personal information, thereby supporting data minimisation and reducing the risks associated with disclosure.
- Credentials that allow individuals to disclose only specific attributes required for a transaction, rather than the full underlying identity dataset, thereby operationalising data minimisation.
- Verification methods that enable a relying party to be satisfied that a condition is met without receiving any of the underlying personal information, thereby significantly reducing disclosure risk.

Part Four: A Department-produced credential

19. Would you support a proposal for the Department to produce an identity credential? Why/why not?

The Law Society supports, in principle, the Department issuing verifiable credentials, provided that this is:

a) strictly voluntary for users;

b) subject to clear statutory and governance frameworks; and

c) carefully scoped to avoid the development of a de facto universal identifier.

20. What do you see as the costs and benefits of a Department-produced credential?

Benefits:

- improves user control and privacy;
- reduced data sharing / enabling data minimisation; and
- enhances efficiency and strengthens trust in the digital identity ecosystem.

Costs/risks:

- concentrates responsibility on the Department;
- potential system-wide impacts of failure and fragmentation if standards are not adopted widely; and
- risk of function creep towards being the de facto national identifier.

Part Five: Sharing

21. What are the minimum 'must have' controls/evidence that should be required before the Department is confident that a third party should be allowed to handle/consume a Department credential?

    a. Should access to sensitive credential attributes require demonstrated capability (training/certification) for third-party personnel? If yes, what should be mandatory?

The Law Society considers that sharing of identity information in a decentralised system must be subject to strict and enforceable controls. Minimum requirements should include:

- appropriate accreditation or assurance thresholds;
- strict purpose limitation and non-retention expectations;
- robust security and privacy protections; and
- contractual (enforceable) acceptance of audit and compliance mechanisms.

The Law Society supports training and certification for third parties accessing sensitive attributes, especially for high-risk sectors (e.g. finance, health, vulnerable populations).

22. What visibility should the Department require (e.g., onward sharing, incident reporting) to maintain confidence in a decentralised ecosystem?

    a. Should the Department require that any subcontractors/downstream parties handling Department credential data meet the same conditions as the primary provider? What visibility should the Department require across the supply chain?

It is essential that any obligations imposed on primary service providers extend to subcontractors and downstream entities, with full transparency across the supply chain. The Department should require:

a) mandatory incident reporting;

b) transparency over onward sharing; and

c) full flow down obligations across subcontractors.

23. If the Department were to produce a credential, what safeguards should there be when that information is shared? Is there any information that we currently hold that should not be credentialised?

The Department should encourage derived attributes over raw data. The Department should restrict credential types based on risk classification, with a strong preference for selective disclosure mechanisms.

Certain information (particularly highly sensitive biometric data or identity data, where misuse risk outweighs utility) may not be appropriate for credentialisation, or should be subject to enhanced restrictions.

24. If a third party fails to meet expectations (assurance, incident response, retention), what consequences should apply (e.g., suspension, revocation, limitation to low sensitivity attributes) and who triggers them?

The Law Society considers that a clear, graduated enforcement framework will be essential to maintaining trust and accountability within a centralised digital identity ecosystem. Consequences for non-compliance should be proportionate to the nature and severity of the failure, and may include:

a) remediation orders for minor or technical non-compliance, requiring prompt corrective action;

b) restrictions on use (such as limiting access to lower-sensitivity attributes only);

c) suspension of access;

d) revocation of access; and

e) in appropriate cases, referral to the Privacy Commissioner or other relevant regulatory authority.

Immediate suspension should be available where there is significant risk of harm.

The Law Society considers that responsibility should be shared but clearly defined:

- The Department, as issuer and system steward, should have the ability to impose operational consequences (including suspension or limitation of credential use).
- The Trust Framework Authority should play a role where non-compliance relates to accreditation standards or systemic assurance failures.
- The Privacy Commissioner should retain oversight in relation to statutory privacy obligations, including investigation and enforcement under the Privacy Act 2020.

In practice, this supports a multi-layered enforcement model, where technical and access controls are managed by the Department, ecosystem integrity is overseen by the Trust Framework Authority, and legal compliance is enforced through existing regulatory mechanisms.

25. Should the Department restrict information sharing with third parties?

    a. Should the Department block identity information we hold (or a credential we have produced) from being shared with a person or organisation that is not accredited under the Trust Framework?

    b. Is there any specific information that should not be shared for the purpose of being credentialised? If so, why?

    c. What is the best way to be able to achieve this?

The Law Society considers that a risk-based, tiered approach should apply, with sensitive credentials restricted to accredited parties, certain high-risk data excluded from credentialisation, and controls implemented through a combination of technical design, accreditation, contractual obligations, and regulatory oversight.

26. Are there other future models for sharing digital identity information you can identify that could better preserve privacy and security for the identity information that the Department handles?

The Law Society considers that there are a number of emerging models for sharing digital identity information that have the potential to better preserve privacy and security than traditional data-sharing approaches. These models are generally characterised by

reducing or eliminating the need to disclose underlying personal information, and by embedding privacy protections into system design:

a) Selective disclosure credentials;

b) Privacy-preserving verification and computation;

c) Zero-knowledge verification techniques (where appropriate);

d) Access-based verification models; and

e) Federated identity verification models.

Future sharing models should prioritise minimal disclosure, user control, and verification without transfer, supported by technical design and enforceable governance frameworks.

Part Six: Disposal

27. If third parties hold or use our information, is there value in considering placing the same requirements on those parties as the Department when handling digital identity information?

The Law Society considers that effective disposal obligations are essential to maintain system-wide integrity and trust in a decentralised system. Third parties handling Department-derived identity information should be subject to disposal obligations equivalent to those of the Department, including compliance with IPP9.

28. Are there additional disposal considerations that the Department will need to consider under a decentralised model (e.g., do we have a responsibility for when we are disposing of information that that information is similarly disposed of elsewhere?)? Is that possible using credentials? Is that wanted?

The Law Society recognises the practical limits on the Department's ability to ensure downstream deletion. A combination of legal, contractual, and technical measures will be required, including:

- clear deletion and retention requirements;
- audit and assurance mechanisms;
- time-limited or revocable credentials where feasible.

A shared responsibility model is appropriate, with the Department responsible for system design and controls, third parties responsible for compliance, and regulators responsible for oversight.

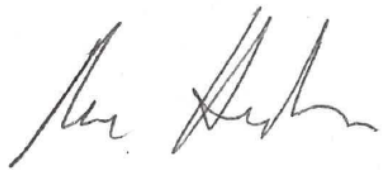
29. Are there other future models for disposing of digital identity information you can identify that could better preserve privacy and security for the identity information the Department handles?

- Credentials that are designed to expire automatically after a defined period or use, thereby limiting the duration for which identity information can be relied upon and reducing the risks associated with ongoing retention or misuse.
- Credentials that can be invalidated by the issuing authority where they are no longer accurate, have been compromised, or should no longer be relied upon, thereby ensuring the ongoing integrity of the identity system.
- System designs that avoid or limit the long-term retention of identity information, instead enabling verification to occur without creating persistent datasets, thereby reducing exposure to security and privacy risks.

Next steps

We hope this feedback is useful, and welcome the opportunity to review proposals in more detail as they are developed. Please feel free to get in touch with us via the Law Society's Senior Law Reform and Advocacy Advisor, Claire Browning (claire.browning@lawsociety.org.nz) if you have any questions or wish to discuss this feedback further.

Nāku noa, nā



Misha Henaghan
Vice President