



18 September 2026

**Re: Privacy Reform - Consultation on Exposure Draft Privacy Amendment
(Personal Data Protection) Bill 2026**

Dear Sir/Madam

The Australian Digital Trust Community Group (ADT CG) under the OpenID Foundation (OIDF) welcomes the opportunity to comment on the consultation to modernise and strengthen Australia's privacy laws.

On a general note, the ADT CG encourages the Australian Government to continue to focus on interoperability and leveraging existing capability when it comes to technical implementation to support legislation. OIDF standards like OpenID for Verifiable Presentation, OpenID for Verifiable Credential Issuance, OpenID Connect, FAPI 2.0, OpenID Federation, Shared Signals are likely to underpin or play a growing role in securing infrastructure in Australia and other nations.

We encourage the Australian community to use the freely available open source tests for implementers to prove out their deployments meet the security, privacy, interoperability and scale properties inherent in the specifications. Should the Australian Government establish an accreditation or conformance scheme that includes (but may not be limited to) OIDF specifications, consider leveraging the low-cost self-certification program (<https://openid.net/certification/>) or the future accreditation program launching in Q2 2026 (<https://openid.net/oidf-announces-new-investment-to-expand-conformance-services/>). Both services are available to ecosystems, with a goal of ensuring ecosystem partners can achieve their objectives.

As a global open standards body, we welcome the opportunity to support the Australian community. As per OIDF's practice of being transparent and open, we intend to share our response to this request for comments in a blog post on openid.net in the near future.

We welcome the opportunity to discuss our comments or other related matters. Please contact David Hyland (dave@idpartners.com.au) regarding any follow-up to this response.

Sincerely

A handwritten signature in blue ink, appearing to read 'J. Scullen'.

John Scullen

on behalf of the Australian Digital Trust Community Group co-chairs

About the Australian Digital Trust Community Group

The Australian Digital Trust Community Group (ADT CG) is a community group of the OpenID Foundation. It is a neutral forum for practitioners working on Australian digital identity and trust services. Members come from technology vendors, banks and other industry sectors, consumer groups, and federal and state government. The group's purpose is to increase awareness and uptake of interoperable, standards-based digital trust services in Australia.

This submission addresses the practical operation of the Bill for identity providers, wallet providers, credential issuers, verifiers and brokers operating under Australian trust schemes. It does not address direct marketing, research or large digital platform provisions.

1. Pseudonymous identifiers and the fair and reasonable test

Section 6FD Note 1 lists a pseudonym or identifier as information that can make an individual reasonably identifiable. Section 6FF makes an individual reasonably identifiable where the information can be combined with other reasonably available information.

Australian identity schemes issue pairwise pseudonymous identifiers. A pairwise pseudonymous identifier is a subject identifier that is different for each relying party, so two relying parties cannot match records by comparing identifiers. The consultation paper says the reasonably identifiable test considers technical feasibility, the cost of identification, and controls on re-identification. The Bill text does not say this.

Request: state in the Bill or the Explanatory Memorandum that a pairwise pseudonymous identifier that the recipient cannot resolve contributes to meeting the data minimisation factor in APP 3.2(d). This matches the position the Court of Justice of the European Union took in *EDPS v SRB* (C-413/23 P, 4 September 2025), where pseudonymised data was held not to be personal data for a recipient with no reasonable means of re-identification, and the approach in NIST SP 800-63C-4, which directs identity providers to use pairwise pseudonymous identifiers to prevent tracking across relying parties.

2. Biometric information and the strictly necessary exception

Section 6FE(d) and (e) make biometric information used for automated verification, and biometric templates, sensitive information. APP 4.1 requires consent to collect them. APP 4.4 removes the consent requirement where collection is strictly necessary to deliver a requested service.

Two specific cases need separating. In the first, a passkey or device authenticator matches a face or fingerprint on the device and the template never leaves the device. The relying party receives a biometrically verified cryptographic signature but no biometric information. In the second, a service captures a face image, sends it to a verification service and matches it against a document photo. The consultation paper's statement that consent is required for biometric templates collected by wearables does not distinguish between these two cases.

Request: confirm that the first case is not a collection of biometric information by the relying party, and provide a worked example for the second case under APP 4.4. Regulation (EU) 2024/1183 (eIDAS 2.0) and NIST SP 800-63B-4 both treat device-bound authentication as the baseline for high assurance, so clarity here affects which authenticators Australian schemes can deploy.

3. Selective disclosure and APP 3.2

APP 3.2(d) asks whether the purpose could be met with less personal information. APP 3.2(e) asks whether the individual has genuine choice.

Selective disclosure is the presentation of a subset of the claims in a credential, with the rest withheld. It is a standard feature of the credential formats used in Australia (ISO/IEC 18013-5 mDL/mdoc and SD-JWT VC, both under OpenID for Verifiable Presentations). Recital 59 of Regulation (EU) 2024/1183 makes selective disclosure a design feature of the European Digital Identity Wallet for the same data minimisation purpose.

Request: name selective disclosure in OAIC guidance on APP 3.2(d) as a recognised means of meeting the factor, so that entities adopting it have a documented basis.

4. Controllers and processors in identity schemes

Section 16D defines a processor as an APP entity acting on a controller's documented written instructions. Section 6A(2A) relieves the processor of the APPs other than APP 1 and APP 11. Section 16D(2) attributes the breach to the controller.

An identity transaction involves at least three parties: the individual, an identity provider or wallet, and a relying party. A broker or scheme operator often sits between them. Each party determines its own purpose for part of the transaction. The Bill does not say which of them is the controller for the disclosure of an attribute.

The definition applies only where both parties are APP entities. A wallet vendor or verifier service under the small business threshold cannot be a processor under section 16D. The controller then carries the obligation with no processor on the other side.

Request: provide worked examples in the Explanatory Memorandum for identity provider, wallet provider, broker and verifier service roles, and address the small business case. The UK Data (Use and Access) Act 2025 Part 2 handles this by certifying digital verification service providers against a trust framework, which gives relying parties a documented basis for the provider's role.

5. Trade and scheme fees

Section 6FC(1) makes a disclosure for money or other consideration a trade. APP 4.2 requires consent to trade. Section 6FC(2)(a) excludes a disclosure made so the recipient can provide a service the individual requested. The consultation paper adds that this covers a commission received by the discloser.

In Australian schemes the relying party often pays the identity provider through a scheme operator rather than directly. The identity provider receives consideration and the individual has requested a service from the relying party, not from the identity provider.

Request: confirm that 6FC(2)(a) covers a disclosure by an identity provider where the fee is paid by or through a third party and the requested service is provided by the recipient.

6. Fraud signal exchange

Section 6FC(3) excludes fraud-related disclosures from trade. Permitted general situation item 2 covers collection, use and disclosure where the entity has reason to suspect serious wrongdoing relating to its functions.

Scheme participants exchange fraud signals about compromised credentials and accounts. The OpenID Shared Signals Framework and CAEP are the standards used. In that exchange the sending party often has no suspicion of its own about the individual concerned. It forwards a signal it received.

Request: confirm that PGS 2 and 6FC(3) cover multilateral signal exchange within a scheme where the sender's reasonable belief rests on the scheme's fraud function rather than on its own investigation.

7. Interaction with the Digital ID Act 2024

The Bill does not mention the Digital ID Act 2024. Accredited entities under the Digital ID Act carry the privacy safeguards in its Chapter 4. Private schemes outside AGDIS carry the APPs only. After this Bill, accredited entities will carry both sets of obligations with no stated order of precedence.

Request: state in the Bill how APP 3, APP 4 and section 16D apply to an accredited entity acting within AGDIS, and whether compliance with a Chapter 4 safeguard satisfies the corresponding APP.

8. Consent and per-scope authorisation screens

Section 6AAB requires consent to be voluntary, informed, current, specific and unambiguous. The consultation paper says bundled consent is unlikely to be voluntary.

OAuth 2.0 and OpenID Connect authorisation screens present the individual with a list of requested scopes or claims and one approve action. The Consumer Data Right consent standards use the same pattern. A 2026 study in Computers & Security found that 35 per cent of private OpenID providers surveyed offer per-claim selection on the consent page.

Request: confirm that a single approve action over an itemised list of claims is not a bundled consent, and state whether per-claim selection is expected.

Follow-up

Contact David Hyland (dave@idpartners.com.au) on behalf of the Australian Digital Trust Community Group