NableU

Curiosity into capability

Submission on the Privacy Amendment (Personal Data Protection) Bill 2026

Practical privacy control for people, sensitive information and AI

Attorney-General's Department consultation | NableU Community Systems Incorporated | INC2601035 | September 2026

Privacy is not meaningful control if a person cannot understand the permission, distinguish the purposes or withdraw it in practice.

NableU Community Systems Incorporated supports the overall direction of the Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026, particularly the proposed statutory consent test, the fair and reasonable test for collection, use and disclosure, clearer controller/processor responsibilities and stronger lifecycle obligations.

Our central concern is practical control. Privacy reform should not stop at technically valid notices, consent records or privacy policies. A person cannot meaningfully control information if they cannot understand the permission, distinguish the purposes, know what happens downstream or withdraw the authority in practice.

NableU works at the intersection of disability, neurodivergence, sensitive support information and governed AI. We recommend five principles.

1. Make valid consent cognitively accessible

We support requiring consent to be voluntary, informed, current, specific and unambiguous. "Informed", however, should not be satisfied merely because complex legal text was presented somewhere in a notice.

Where handling involves sensitive information, health or disability information, financial information or AI processing, entities should take reasonable steps to make the decision usable: layered notices, plain language, clear choices, accessible formats, separation of optional purposes and enough information to understand the consequences of refusing.

This is especially important for people with cognitive, communication or executive-function disabilities. Formal equality of presentation does not guarantee equal ability to make an informed choice.

2. Keep the fair and reasonable test independent of consent

NableU strongly supports the proposed fair and reasonable requirement. Consent should not operate as a waiver that makes an otherwise excessive practice acceptable.

The proposed test appropriately directs attention to matters such as reasonable expectations, transparency, data minimisation, genuine choice, privacy impact and proportionality. Those factors are particularly important where there is a power imbalance or practical dependence. A person may "agree" because refusal means losing access to a service, job, platform or support pathway.

The central question should remain whether the handling is justified and proportionate for the purpose, not merely whether an organisation obtained a click or signature.

3. Treat inferred and AI-generated information as real personal information

Modern systems do not only collect information supplied by a person. They create classifications, predictions, risk signals, behavioural profiles and other inferences from existing data.

The OAIC's updated APP 3 guidance states that where an entity creates personal information with reference to, or generated, inferred or observed from, other information it holds, that is itself a collection of personal information.

This principle should remain clear in the reforms. A false inference can be more consequential than the raw data from which it was produced. Where inferred information materially affects a person, they should be able to know it exists, correct relevant source data and challenge materially inaccurate or misleading profiles used in significant decisions.

4. Do not make meaningful privacy rights depend mainly on entity size

The proposed right to erasure for large digital platforms is a useful step, but the underlying interest - ending unnecessary retention of personal information - is not unique to very large platforms.

A small organisation may hold highly sensitive disability, health, safeguarding, financial or intimate information. The risk to the individual depends on the information, purpose, retention and consequences, not simply the revenue or user count of the entity holding it.

NableU supports proportionate compliance obligations for smaller entities. But proportionality should usually change how an obligation is implemented, not whether an individual has meaningful privacy rights at all. Government should continue toward broader retention and erasure rights based on necessity, lawful retention obligations, sensitivity and risk.

5. Separate AI permissions and preserve controller accountability

AI makes bundled privacy concepts particularly dangerous. These are different decisions:

- may the organisation store the information?
- may another person or organisation receive it?
- may AI use it as context for a particular task?
- may it persist as AI memory?
- may it be used for model training or evaluation?
- may an AI system act on the person's behalf?

Permission for one should not silently imply the others.

Where an organisation uses an AI, cloud or other processor, the controller should remain clearly accountable for why the information is processed, what enters the processor, the permitted purpose, retention, onward disclosure, security and whether the processor may use the information for its own training or secondary purposes.

Revocation should also have operational meaning. Where consent is the legal basis and it is technically feasible, withdrawing permission should stop new access and new processing under that authority promptly rather than applying only to a future policy cycle.

Implementation for small organisations

NableU is itself a small community organisation. Stronger privacy obligations can create genuine implementation burden. The answer should be proportionate, reusable compliance infrastructure rather than broad exemptions for organisations handling highly sensitive information or high-impact AI.

Government and the OAIC should provide practical templates for privacy impact assessments, processor clauses, retention schedules, consent patterns, data inventories and AI processing permissions. That would make strong individual rights achievable without requiring every community organisation to build an enterprise legal function.

Conclusion

The Exposure Draft is strongest where it moves Australian privacy law away from formal notice-and-consent mechanics toward substantive fairness, reasonableness, minimisation and accountability.

NableU recommends carrying that logic through consistently. Privacy should give people practical control over how information about them is collected, inferred, used, retained, shared and passed into AI systems.

If a person cannot understand the permission, distinguish the purposes or meaningfully withdraw it, the system should not treat the existence of consent as proof of meaningful control.

Principal sources

Attorney-General's Department, Privacy Reform - Consultation on Exposure Draft legislation, opened 31 August 2026.

Attorney-General's Department, Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026 and accompanying Consultation Paper.

Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines - APP 3: Collection of solicited personal information, updated 13 May 2026.

Office of the Australian Information Commissioner, guidance on privacy and commercially available AI products, and guidance on consent.

NableU supports publication of this submission and the organisation name. Direct contact details may be withheld from publication.