

Privacy Act Reforms Tranche 2

The Australian Government has released an [Exposure Draft](#) of the Privacy Amendment (Personal Data Protection) Bill 2026, accompanied by a [Consultation Paper](#). This tranche of reforms has around 40 proposals, arguably representing the most substantial rewrite of Australia's privacy framework in over a decade.

25 Privacy Act Review proposals
uplifting privacy protections

5 Privacy Act Review proposals
clarifying and simplifying obligations

4 Additional measures to simplify
existing obligations

7 Additional measures to improve
efficiency of the Office of the Australian
Information Commissioner (OAIC)

Several of the proposals would require organisations to rebuild core compliance processes rather than simply update a policy document. A live planning exercise should commence now in light of the sweeping proposals.

Headline Changes

A new "fair and reasonable" test for APP 3:

This is the centrepiece of the package and represents a significant shift in how privacy obligations are framed.

Lengthy privacy notices and consent-heavy compliance models will no longer be enough on their own. Organisations must show that their data handling is objectively fair and reasonable in the circumstances, assessed against legislated factors including reasonable expectations, connection to the entity's functions or activities, transparency, data minimisation, genuine choice, privacy impact and risk of harm to the individual, and the best interests of the child (if applicable).

Strengthened data breach obligations:

The NDB scheme is materially tightened. Entities must notify the Information Commissioner within [72 hours](#) of becoming aware of reasonable grounds to believe an eligible data breach has occurred, with ongoing obligations to provide updated information where necessary. This is in addition to the existing requirement to complete an assessment within 30 days.

Separately, a new concept of "data breach" is introduced (as distinct from an "eligible data breach"), with positive obligations to maintain practices, procedures and systems enabling an effective breach response, and to take reasonable steps to mitigate harm as soon as there are reasonable grounds to suspect a data breach, not only once an eligible breach is confirmed.

Right to erasure on large digital platforms (new APP 14):

Large digital platforms meeting the gross revenue or number of end-user thresholds must destroy personal information on request, subject to limited exceptions. This signals a clear regulatory expectation that individuals should have ongoing control over their personal information, not merely a one-time notice at the point of collection.

Modernised core definitions:

Updates for a range of key concepts have been proposed (including the below), pointing to a need to revisit how data flows through the organisation.

Statutory requirements are proposed for “consent”, being voluntary, informed, current, specific and unambiguous.

The definition of “personal information” is broadened from information “about” to information that “relates to” an identified or reasonably identifiable individual. Information that enables an individual to be recognised, for instance, through a pseudonym or geolocation data, may be considered personal information. Clarity is provided as to what amounts to “reasonably identifiable”, which contemplates a combination of multiple pieces of information or opinion.

Consent to “trade” personal information:

A new concept of “trading” captures disclosures for money, other consideration, or direct marketing purposes (subject to narrow carve-outs). Consent remains relevant where personal information is traded, and this is intended to capture arrangements such as customer list transfers and programmatic advertising processes.

Simplified direct marketing rules:

APP 7 is replaced with a streamlined, technology-neutral framework. Organisations must provide a simple opt-out mechanism and action requests. Ad-supported services may offer different terms to users who opt out, provided those terms give a genuine choice.

Data security and minimisation:

APP 11 is substantially strengthened, requiring entities to consider destruction (not just de-identification), identify the personal information they hold, and regularly evaluate the effectiveness of their security measures.

Controller-processor framework:

A formal controller-processor split is introduced for the first time, aligning Australia's privacy framework more closely with some of its key international counterparts. Generally speaking, where a processor acts on a controller's documented instructions, primary APP compliance sits with the controller (except APP 1 and APP 11). In the context of outsourcing or cloud arrangements, specific written instructions are needed to ensure they fall within this exception.

The Consultation Paper also seeks feedback on whether the reforms adequately address privacy risks from emerging technologies, including wearable surveillance devices and connected vehicles, and in strengthening the OAIC's enforcement powers spanning dispute resolution, complaint handling and investigations.

The direction of travel is clear – the regulatory focus is towards whether underlying data practices are fair, reasonable and subject to proper governance.

If you would like to understand what these changes mean for your organisation, or to make a submission to the Consultation Paper ([due 18 Sep 2026](#)), please get in touch with Candy Lau.

Candy Lau is a Partner at Ironbridge Legal with over 15 years of experience in the industry across APAC.

She advises clients on financial services regulatory compliance, corporate governance, privacy and the Security of Critical Infrastructure regime.

Candy is recognised for her work advising global and domestic financial institutions on regulatory reform and complex remediation programs.

