

September 2026

UPDATE

Privacy Reform Exposure Draft Released

Privacy Amendment (Personal Data Protection) Bill 2026

The [Attorney-General's Department](#) has released an exposure draft of the [Privacy Amendment \(Personal Data Protection\) Bill 2026](#) (Bill) together with a [consultation paper](#). The package is the next stage of privacy reform following the *Privacy and Other Legislation Amendment Act 2024* (Cth) and contains approximately 40 proposals: 30 from the Privacy Act Review Report, 4 additional measures intended to simplify existing obligations, and 7 measures directed at the efficiency of the Office of the Australian Information Commissioner (OAIC).

The Bill repeals and replaces Australian Privacy Principles (APPs) 3, 4, 6 and 7, rewrites APP 5 and APP 11, adds a new APP 14, and changes the definitions of "personal information", "sensitive information", "consent", "collects", "discloses" and "de-identified".

Summary of important changes

1. **A single 'fair and reasonable' test replaces APPs 3, 4 and 6:** An APP entity must not collect, use or disclose personal information unless doing so is fair and reasonable in the circumstances, and lawful. Seven matters must be considered: reasonable expectations, the relationship to the entity's functions or activities, transparency, whether less personal information could be used, genuine choice, the impact on the individual including proportionality, and, for a child's information, the best interests of the child as a primary consideration. Exceptions apply where the handling is required or authorised by law, or a permitted general or permitted health situation exists. The primary purpose and related secondary purpose analysis in current APP 6.2 is removed, although reasonable expectations survive as one of the factors. The requirement that use and disclosure be 'lawful' is new.
2. **Permitted general situations are widened, and so is the ability to act against wrongdoing by third parties:** The permitted general situations in section 16A are restructured into a table of 13 items, and their significance increases markedly under the new framework. A permitted general situation is an exception not only to the requirement for consent to collect sensitive information, but also to the new fair and reasonable requirement and to the requirement for consent to trade. An entity that brings its handling within a permitted general situation is therefore relieved of the central obligation in the Bill, although the separate requirement that collection, use and disclosure be lawful continues to apply.

The substantive change is to item 2, which permits collection, use and disclosure where an entity has reason to suspect unlawful activity or misconduct relating to its functions or activities and reasonably believes the handling is necessary to take appropriate action. Two amendments are made. First, 'misconduct of a serious nature' becomes 'wrongdoing of a serious nature,' which is intended to be broader than misconduct and to reach conduct by a person acting in a private capacity, including some forms of financial abuse. Second, the item is amended to state expressly that the unlawful activity or wrongdoing may be engaged in 'by a person owing a duty to the entity or any other person.' The corresponding ground for refusing access in APP 12.3(h) is amended in the same terms.

The practical effect is to confirm that an entity may collect and use personal information to protect itself, its staff and its customers against wrongdoing by third parties — shoplifters, fraudsters, abusive customers and organised offenders — provided the conduct relates to its functions or activities and the response is proportionate. The consultation paper confirms that the item supports proactive monitoring and risk detection where an entity has reason to suspect fraud or other serious wrongdoing, even if no specific instance has yet been identified. Separately, disclosures made to prevent, detect, investigate or remedy unlawful activity or serious fraud-related wrongdoing are carved out of the definition of ‘trade,’ so they do not attract the new consent requirement.

This is consistent with the outcome in *Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel)* [2026] ARTA 130, decided on 4 February 2026.

3. **Consent is redefined:** Consent must be voluntary, informed, current, specific and unambiguous. On the consultation paper’s account, bundled consents, pre-ticked boxes, preselected settings and interfaces that make refusal unreasonably difficult will not satisfy the definition. Consent is required for the collection of sensitive information and the trading of personal information.
4. **Geolocation and genomic information are sensitive information:** ‘Precise geolocation tracking data’ becomes sensitive information. It is defined as personal information generated by or derived from a device that identifies an individual’s location to within a radius of 500 metres and is collected and held by reference to location over time. Genomic information is also expressly included. Collection of sensitive information requires consent unless an exception applies, including a new exception where collection is strictly necessary to provide a good or service the individual has requested, and a new exception for collection from a ‘publicly available document.’
5. **Consent is required to trade personal information:** Trade is defined as disclosure for money or other consideration, or for the purposes of direct marketing. The consultation paper says that cookies and pixels in programmatic advertising are within scope. Four exceptions apply: disclosure to provide a good or service the individual requested; disclosure incidental to a business transfer, provided disclosure of personal information is not a substantial purpose of the transaction; disclosure by a controller to a processor; and anti-fraud disclosures.
6. **A new direct marketing framework:** Direct marketing is redefined in technology neutral terms and expressly captures selection of an individual as a member of a class using their personal information, which brings audience segmentation and online behavioural advertising within APP 7. Organisations must provide a simple opt-out, take reasonable steps to give effect to opt-out requests, and include opt-out information in every communication. An ‘ad-supported service’ may offer the service on different terms to an individual who opts out, provided those terms give genuine choice — an endorsement of the ‘consent or pay’ model.
7. **Data breach notification must be within 72 hours:** This is in line with the deadline under the Security of Critical Infrastructure Act 2018 (Cth) for an incident having a relevant impact, and with the EU General Data Protection Regulation (GDPR). An entity aware of reasonable grounds to believe an eligible data breach has occurred must give the Commissioner a statement within 72 hours, with a civil penalty for failing to do so. An incomplete statement may be given where a complete one is impossible or impracticable, with the missing matters and material changes to be notified as soon as practicable. Two further obligations apply whether or not the serious harm threshold is met: to implement practices, procedures and systems enabling an effective response, and to take reasonable steps to prevent or reduce harm as soon as practicable after becoming aware of grounds to believe or suspect a breach.

Breach of either is an interference with privacy. The 30-day assessment period for suspected breaches is unchanged.

8. **APP 11 is rewritten:** An entity holding personal information it no longer needs must first consider whether to destroy it, then take reasonable steps to destroy or de-identify it. An entity must take any steps needed to ensure it is able to identify the personal information to which APP 11 applies, and must regularly evaluate the effectiveness of its compliance, including whether de-identified information remains de-identified. In practice this requires a maintained data inventory and a recurring assurance cycle.
9. **Introduction of the concepts of controllers and processors:** Where a processor acts on a controller's documented instructions and for the purposes specified in them, its acts are taken to be acts of the controller and do not breach the APPs other than APP 1 and APP 11. There is no prescribed form of instructions, but they must address the purposes for which the processor will handle the information. A processor acting outside its instructions loses the protection entirely. Both parties must be APP entities, and Commonwealth contracted service providers are excluded.
10. **Collection notices are simplified:** The list of matters in APP 5.2 is repealed and replaced with two: the fact and circumstances of the collection, and the purposes for which the entity intends to use or disclose the information. Notification must be in clear and plain language, readily understandable, up to date and concise, and must be updated when practices change. The existing requirement to identify the countries to which information is likely to be disclosed is removed.
11. **A right to erasure for large digital platforms:** A new APP 14 requires a 'large digital platform' to destroy an individual's personal information on request, subject to exceptions, and to give written notice of the outcome within a reasonable period. An organisation is a large digital platform if it provides a social media service, relevant electronic service or designated internet service under the *Online Safety Act 2021* (Cth) and either its business group had gross revenue of \$500 million or more in the previous financial year, or its platform averaged 2.5 million or more monthly end users in Australia. The revenue test applies to the whole business group including overseas members, so Australian subsidiaries of large foreign groups are caught regardless of local scale.

The Bill also makes the following changes:

Personal information is redefined as information or an opinion that 'relates to' an identified or reasonably identifiable individual, with a note confirming that an individual may be identifiable without their name or legal identity being known. A new definition of 'reasonably identifiable' is inserted.

Collection occurs when an entity collects information for inclusion in a record or generally available publication, regardless of source or means, expressly including information generated or derived by data analysis or artificial intelligence. An entity is not taken to collect sensitive information merely because it collects information from which sensitive information could be derived; timing rules govern when derived sensitive information is taken to be collected.

Disclosure is defined as making personal information accessible to another person or body. Mere transmission or storage, including overseas, is not a disclosure unless the information is made accessible.

De-identified is redefined as a contextual state rather than a fixed one. Information that has been subject to de-identification techniques may remain personal information if an individual is reasonably identifiable through combination with other available information.

APP 12 gains a new exception where, despite reasonable steps, giving access to the personal information of an individual remains unreasonable or impracticable because it is technically impossible or infeasible. The exception applies only to the extent that access is affected, and access must still be given to the balance.

Research exceptions are consolidated. The existing health and medical research provisions are replaced by a single exception for 'human research' reviewed, approved and monitored under the National Statement on Ethical Conduct in Human Research and conducted in accordance with guidelines to be made by the Commissioner. The consent definition is relaxed for such research. Commencement is contingent on the guidelines being made.

Measures foreshadowed without draft provisions

Several measures affecting the OAIC are described in the consultation paper but have not been drafted. Notably:

- **Complaint handling:** Entities would be required to provide accessible complaint mechanisms, respond within 60 days, and give written decisions setting out the outcome and available review options. Breach of these obligations would itself be an interference with privacy, enforceable by civil penalty, infringement notice and compliance notice. Every APP entity would need a compliant complaints process.
- **A power to require reasonable assistance:** Modelled on section 19 of the *Australian Securities and Investment Commission Act 2001* (Cth), the Commissioner could require any person able to assist an investigation to provide reasonable assistance, expressly including access to systems and accounts, backed by a civil penalty and applying to public inquiries as well as investigations. Defences for self-incrimination, legal professional privilege and journalists' sources are foreshadowed.
- **Repeal of section 43(8A).** The current restriction on the Commissioner briefing Ministers about investigations involving most private sector entities would be removed.

What the Bill does not include

The Government's September 2023 Response to the Privacy Act Review Report agreed to 38 of the Report's 116 proposals and agreed in-principle to a further 68. Across both tranches, 50 proposals have now received no legislative response to date. It is notable that removal of the small business exemption, extension of privacy protections to private sector employee records, the rights to object, to de-index search results, and mandatory privacy impact assessments for high privacy risk activities are not included in the Bill.

Submissions are invited by the Attorney-General's Department by 18 September 2026..

Please contact me if you have any questions regarding the matters discussed in this update.

patrick@patrickfair.com 0411361534. You can subscribe to updates like this one at www.patrickfair.com