



Leah Mooney
AI Governance
and Privacy Lead

+61 7 3236 8739
leah.mooney@
wottonkearney.com

Australian Privacy Act Reforms

Second Tranche Privacy Reforms have arrived

On 31 August 2026, the Australian Government released a Consultation Paper and Exposure Draft legislation with the stated aim to 'modernise and strengthen Australia's privacy laws for the digital age.' The package of reforms includes the Exposure Draft *Privacy Amendment (Personal Data Protection) Bill 2026* (**Second Tranche Reforms**). This represents the first significant proposed reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**) since the passage of the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**First Tranche Reforms**) which included the statutory tort for serious invasions of privacy and transparency requirements for automated decisions significantly impacting the rights and interests of individuals.

Related Law Reform

Privacy issues arising from emerging technologies

In addition to the specific measures included in the Second Tranche Reforms, the Consultation Paper is seeking feedback on proposed measures under development to:

- Address privacy issues arising from emerging technologies, including wearable surveillance technologies (such as smart glasses and ear buds) and connected vehicles
- Support the efficient administration and enforcement of the Privacy Act by the Office of the Australian Information Commissioner (**OAIC**), including in the context of early complaint resolution, representative complaints and the privacy protections associated with the Social Media Minimum Age under the *Online Safety Act 2021* (Cth).

The Government also announced the introduction of 'IDLock', a new digital identity protection service designed to give Australians direct control over how their identity documents are used for verification. IDLock, to be made available through myGov next year, will enable individuals to block, unblock and monitor the use of eligible identity documents through the Document Verification Service at any time.

Do Now

Engage with and contribute to the consultation process, including the adequacy of the Second Tranche Reforms to **address emerging tech**

Do Next

- Conduct privacy impact assessments (**PIAs**) before commencing higher risk processing activities, **including implementing AI**
- Review consent management practices to ensure valid consent is obtained

Do Later

- Prioritise data minimisation: map data, capture retention obligations and **securely destroy and de-identifying data no longer required**
- Plan for the impacts of new definitions and data handling requirements, including the proposed fair and reasonable test

Key Reforms

Data Security and breach response

Uplifting obligations when responding to data breaches to minimise the risk of harm to individuals and ensure timely and informative notifications. Reforms include:

- Introducing a **72-hour notification period for advising the Information Commissioner** of eligible data breaches
- Requiring entities to implement proactive steps to enable effective breach response and mitigate harm to individuals
- Further strengthening and clarifying the security of personal information provisions in APP 11 by introducing requirements to consider destruction of personal information an entity no longer requires (**data minimisation**), identify the personal information it holds (**data mapping**) and **regularly evaluate the effectiveness of its security measures**

Strengthening handling, consent and notice requirements

Proposed personal information handling requirements will be simplified, centered around a new fair and reasonable test. Reforms include:

- Replacing existing APPs 3, 4 and 6 with a new framework permitting collection, use and disclosure only when the **new fair and reasonable test** is satisfied
- Requiring **valid consent** to collect **sensitive information** or **trade in personal information**, unless an exception applies
- **Simplifying notification requirements** when collecting personal information.
- Replacing APP 7 with a **simplified direct marketing framework**

Right to erasure, data controllers and processors

Introducing new rights and concepts aligning with international privacy laws including:

- A new right to erasure on large digital platforms, including social media
- Introducing the concept of, and allocating responsibility between, data controllers and processors

Uplifting core definitions

Updating and clarifying core Privacy Act definitions to better reflect contemporary digital environments, data practices and community expectations including:

- Extending the definition of **'personal information'** to cover information that 'relates to' an individual and creating a new definition of **'reasonably identifiable'**
- Expanding the definition of **'sensitive information'** to recognise new categories warranting additional safeguards, **including 'precise geolocation tracking data'**
- Clarifying when 'de-identified' data may remain personal information
- Confirming when personal information is **'collected'**, including specific circumstances for 'sensitive information' and AI generation
- Providing greater clarity on when personal information is **'disclosed'**, including where it is transmitted or stored overseas
- Requiring that valid **'consent'** must be voluntary, informed, current, specific, and unambiguous