

2025 KEY DATA AND PRIVACY DEVELOPMENTS

The Australian Government is changing the law to protect consumer privacy after a series of high-profile data breaches, and to align the law with safer and more protective laws in other regions. This fact sheet outlines the key reforms passed in the first tranche of legislation.

| legalvision.com.au | info@legalvision.com.au | 1300 544 755

KEY REFORM #1: AUTOMATED DECISION TRANSPARENCY



Organisations must provide greater transparency when using personal information for automated decisions.

- Applies to decisions that may significantly affect individuals' rights or interests.
- Includes decisions about benefits, contractual rights, or access to significant services or support.

KEY REFORM #4: CHILDREN'S ONLINE PRIVACY CODE



To be developed and registered by the Australian Information Commissioner within 24 months. Will:

- apply to services likely to be accessed by children, including social media, messaging, gaming, and general websites.
- align with similar regulations in other jurisdictions, such as the UK's Age Appropriate Design Code.

KEY REFORM #2: ANTI-DOXXING OFFENCES



Introduces new criminal offences for using a carriage service to maliciously publish or distribute personal data.

- Maximum penalties of 6-7 years' imprisonment, with higher penalties for targeting based on protected attributes.

KEY REFORM #5: OVERSEAS DATA SHARING



Allows the government to officially recognise countries and certification schemes with privacy protections similar to Australia's.

- Aims to simplify international data sharing for organisations.

KEY REFORM #3: NEW RIGHT TO SUE FOR PRIVACY



Individuals can now sue for serious invasions of privacy and personal information misuse.

- Courts will balance privacy rights against public interest considerations.
- Damages may be awarded for emotional distress, with caps on non-economic and exemplary damages.

KEY REFORM #6: ENHANCED ENFORCEMENT POWERS



Provides the Australian Information Commissioner with new mid- and low-tier civil penalty provisions.

- Maximum penalty for mid-tier breaches: \$3.3 million for companies.
- Grants powers to issue infringement notices up to \$330,000 for companies for certain administrative breaches.

2025 KEY DATA AND PRIVACY DEVELOPMENTS

BACKGROUND



- In February 2023, the Attorney-General's Department released its Privacy Act Review Report 2022, proposing further changes to the *Privacy Act 1988* (Cth).
- In September 2023, the Australian Government released a response to the Report, revealing the changes likely to be made to privacy laws in 2024.
- The *Privacy and Other Legislation Amendment Act 2024* (Cth) passed both Houses of Parliament on 29 November 2024, received Royal Assent on 10 December 2024, and is now in effect, representing the most substantial change to Australia's privacy regime since its inception.

IMPLEMENTATION TIMELINE



- Most changes took effect immediately on 10 December 2024.
- The law allowing people to sue for serious privacy invasions will start by 10 June 2025 at the latest.
- Enhanced transparency requirements for automated decisions have a two-year grace period, ending 10 December 2026.

STEPS YOU SHOULD TAKE



- Review and update your privacy policies and procedures to align with the new requirements.
- For services accessible by children, prepare for the Children's Online Privacy Code.
- Assess your automated decision-making processes and plan for enhanced transparency measures.
- Incorporate the new information-sharing framework into data breach response plans.
- Understand the new enforcement powers and ensure compliance to avoid penalties.
- Train staff on the new privacy obligations, particularly handling personal information.
- Seek legal or expert advice to ensure full compliance with the new privacy landscape.

POTENTIAL FUTURE REFORMS



- Expand the definition of personal information to include online identifiers.
- Remove or narrow the small business and employee records exemptions.
- Introduce new individual rights, such as the right to erasure and search result de-indexing.
- Implement stricter rules for direct marketing and targeted advertising.
- Introduce a 'fair and reasonable' test for handling personal information.
- Shorten the timeframe for reporting data breaches from 30 days to 72 hours).
- Distinguish between data controllers and processors per the EU's GDPR.