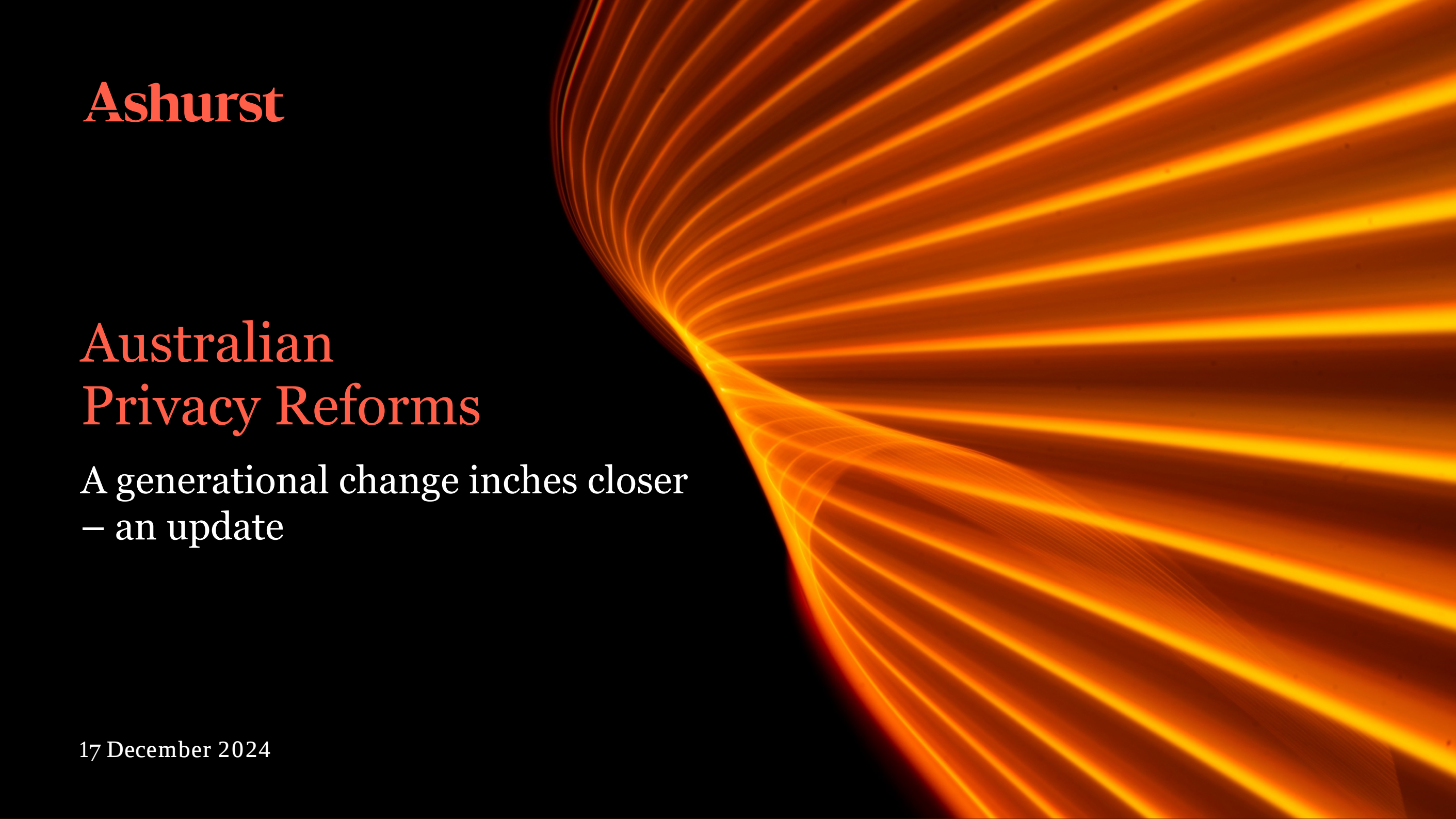




Ashurst

Australian Privacy Reforms

A generational change inches closer
– an update

17 December 2024

The first brick in the wall

The Australian Government has launched its next round of proposed privacy reforms, aimed at ensuring that **the Privacy Act is fit for purpose in the digital age**. Proposed changes will be introduced in two tranches:



What reforms have been introduced?



23 of the proposals that were ‘agreed’ in the Government Response to the Privacy Act Review (September 2023), out of total of 116 proposals.

- Enhanced regulator powers** – with a new menu of investigation and enforcement options, including search and seizure powers, infringement notice powers, and tiered penalties.
- Automated decision-making/AI** – new transparency requirements, a first step in broader automated decision-making and AI reforms.
- Cybersecurity uplifts** – enhanced information security obligations, with greater information sharing rights, and tools to respond to data breaches.
- Code-making framework and Children’s Online Privacy Code** – the first cab off the rank under a stronger code-making framework for the OAIC.
- Simpler international data transfers** – allowing the regulations to prescribe countries and binding schemes with ‘substantially similar’ privacy protections.
- Statutory tort** – a long-awaited right to make a claim for intentional or reckless serious invasions of privacy brings Australia closer to international regimes, and opens new avenues for litigation and potential class action risk.
- Anti-doxxing** – broad criminal offences for exposing personal data in a way that is menacing or harassing, capturing the intentional and malicious exposure of personal data online.

Commencement

Applies now

24 months (11 Dec 2026)

Applies now

Applies now (Code to be registered by 10 Dec 2026)

Applies now (but needs regulation)

On proclamation or 11 Jun 2025

Applies now

New items that were introduced



A handful of last-minute changes were introduced in the final version of the bill, including:



Compliance notices – the addition of a new power for the Information Commissioner to issue a discretionary notice to an entity to remedy an alleged breach of specified provisions.



Review of operation of the doxxing offence – independent review of the doxxing offence within 24 months, with a report due 6 months later.



Changes to the statutory tort – a new limb for the statutory tort, specifically requiring a balancing of public interest in a plaintiff’s privacy against countervailing public interests (including freedom of expression, political communication, artistic expression, among others), a right to seek a determination from the court on any exemptions, and tweaks to the definition of journalistic material, and a new ‘good faith’ exemption from the statutory tort for government agencies.



Other changes – minor amendments to emergency declarations (relating to the ABC and the SBS), the Childrens Online Privacy Code submission timeframe, and to the operation of eligible data breach declarations (to exclude media organisations, the ABC and the SBS).

Next steps for the reform pathway:

Tranche 1 reforms have passed:

- *Privacy and Other Legislation Amendment Act 2024* was passed on 29 November 2024, receiving assent 10 December 2024.
- Tranche 2 consultation to come.

Consultation on Tranche 2:

- Broad spread of reforms – including a new “fair and reasonable” requirement, consent reforms, individual rights, small businesses and employee exemptions, and assessing the privacy impact of high-risk activities.
- May be delayed if an election is called

Part of an ambitious and interconnected digital reform agenda

Alongside privacy reforms, the Government has progressed:

Social media ban – for under 16s, to be implemented by social media platforms. by a date to be proclaimed (but before 11 December 2025).

Hate crimes – expanded offences for urging, or directly threatening, violence against particular groups. Bill is currently before Parliament.

Cyber security – new laws have been passed, including ransom payment reporting and mandatory standards for digitally-connected devices.

Security of critical infrastructure – reforms have passed, including a focus on data storage systems and telecommunications.

The two things to do to reduce your risk and increase customer trust:

The proposed changes materially increase your risk by introducing a wider toolbox of regulator enforcement options and a statutory tort for serious invasions of privacy. This puts the onus on your practices, procedures and systems to provide a defensible position for collection, use, and disclosure.

Uplifting practices, procedures, and systems

1

Current State Assessment

Conduct an assessment to evaluate the effectiveness of your current privacy risk management framework, including PIAs, privacy by design, third-party risk and roles and responsibilities allocation, legal obligations, and where gaps exist

2

Gap Analysis

Identify the gaps between your current state and your new obligations under the reforms and where you may need to uplift your practices, procedures, and systems

3

Uplift to new standard

Develop a plan to remediate any gaps between your current state and your internal and external practices, procedures, and systems to understand and manage your privacy risks

Automated decision-making

1

Identify legal and risk obligations

Privacy Act obligations (as well as new AI guardrails) need to be understood to define the scope of work. The obligations will guide the risk scope of work to control the risk

2

Map use cases and personal information

Develop a plan to identify any use cases of automated decision-making and AI in the business. A use case review should be undertaken to determine if each requires risk assessment. Personal information used and created must be mapped for each use case

3

Monitor and Review

Privacy risk management is not a one-off exercise – it requires constant monitoring and review to ensure the ongoing mitigation of emerging risks and uplift to the new privacy obligations in Tranche 2 of the Privacy Act reforms and other AI guidance

Getting the foundations right will give you an advantage

Ensuring you have the practices, procedures and systems in place and helping you outpace change

The privacy reforms mark the beginning of **significant changes in Australian privacy law**, increasing the risk for businesses in the digital economy.

Business leaders who adapt effectively to these changes by **implementing reliable and provable privacy practices, procedures, and systems** can mitigate risks and gain a competitive edge through enhanced customer trust.

Ashurst offers comprehensive support in data privacy and risk management, leveraging legal and risk advisory expertise to help clients **achieve operational resilience and compliance.**

Privacy



[Geoff McGrath](#)
Partner
Digital Economy



[Emma Butler](#)
Practice Group Head
Digital Economy



[Chris Baker](#)
Partner, Regulatory
Risk & Privacy
Risk Advisory



[Leon Franklin](#)
Director
Privacy
Risk Advisory

Cyber and data risk



[John Macpherson](#)
Partner
Cybersecurity
Risk Advisory



[Sonia Haque-Vatcher](#)
Partner
Data and Analytics
Risk Advisory

This publication is a joint publication from Ashurst Australia and Ashurst Risk Advisory Pty Ltd, which are part of the Ashurst Group.

The Ashurst Group comprises Ashurst LLP, Ashurst Australia and their respective affiliates (including independent local partnerships, companies or other entities) which are authorised to use the name "Ashurst" or describe themselves as being affiliated with Ashurst. Some members of the Ashurst Group are limited liability entities. The services provided by Ashurst Risk Advisory Pty Ltd do not constitute legal services or legal advice, and are not provided by Australian legal practitioners in that capacity. The laws and regulations which govern the provision of legal services in the relevant jurisdiction do not apply to the provision of non-legal services. For more information about the Ashurst Group, which Ashurst Group entity operates in a particular country and the services offered, please visit www.ashurst.com.

This material is current as at 17 December 2024 but does not take into account any developments after that date. It is not intended to be a comprehensive review of all developments in the law or in practice, or to cover all aspects of those referred to, and does not constitute professional advice. The information provided is general in nature, and does not take into account and is not intended to apply to any specific issues or circumstances. Readers should take independent advice. No part of this publication may be reproduced by any process without prior written permission from Ashurst. While we use reasonable skill and care in the preparation of this material, we accept no liability for use of and reliance upon it by any person.