September 2024

Tax and Compliance Alert

Privacy and Other Legislation Amendment Bill 2024 Introduced

At a glance

- First tranche of Privacy Act 1988 reforms introduced into Parliament.
- Will enhance privacy protections for individuals.
- Reforms only partially address expected changes; further significant reforms are anticipated in a forthcoming second tranche.
- Key features of the Bill.
- What the changes mean.
- Actions to consider now.
- How EY can help.

On 12 September 2024 the Australian Government introduced the first tranche of reforms to the Privacy Act 1988 (Cth) (Privacy Act), into Parliament, in the Privacy and Other Legislation Amendment Bill 2024 (the Bill).

The Bill is the latest development in a four year long process following a review by the Attorney General's Department, stakeholder consultation and the Government's response. If enacted, the Bill will enhance privacy protections for individuals by:

- Granting the Office of the Australian Information Commissioner (the independent national regulator for privacy and freedom of information) greater enforcement powers
- Establishing a right for individuals to sue for serious privacy breaches
- Mandating clearer disclosures about the use of personal information in automated decision-making
- Strengthening privacy safeguards for children
- Criminalising the act of doxing to deter the malicious sharing of personal information online.

In response to polling conducted by the Information Commissioner[1], 89% of Australians indicated they support reform to the Privacy Act to make it fit for the digital age and this is squarely on the Government's legislative agenda. While the Bill introduces some added protections for consumers, this first tranche of reforms only gets us part of the way there. Many of the significant changes expected based on the Government's response to the Attorney General's review have been excluded from this first tranche. These further changes will likely be introduced in future legislative updates following more consultation with stakeholders.

We expect that the Government will introduce further reforms so that Australia can keep up with privacy and data protection laws globally, but it is not yet clear when this will happen.

With a Federal Election approaching in early 2025, the path forward for privacy reform in Australia continues to be unpredictable.

Key features of the Bill

If enacted, as drafted, the Bill would introduce the following changes to the Privacy Act:

- Broader Enforcement Powers for the Australian Information Commissioner: This would likely mean that the Information Commissioner would have increased authority to investigate privacy breaches, enforce

[1]Office of the Australian Information Commissioner (OAIC), "OAIC welcomes reforms critical to Australia's privacy future", 28 September 2023.

compliance with privacy laws and impose penalties on organisations that violate privacy regulations.

- Statutory Tort for Serious Invasions of Privacy: A statutory tort would create a new civil wrong, allowing individuals to sue for compensation if their privacy is seriously invaded without their consent. This could cover a range of actions, including unlawful surveillance, hacking, or the dissemination of personal information.
- Greater Transparency for Automated Decision-Making: This change would require organisations to be more open about how they use personal information to make automated decisions. This could include decisions made by algorithms or artificial intelligence (AI), and the requirement could extend to providing individuals with explanations of how such decisions are made. In parallel the Government has introduced a policy for the responsible use of AI for Federal Government departments and agencies.
- Additional Protections for Children's Privacy: Enhanced protections for children could involve stricter rules on the collection, use, and disclosure of children's personal information, recognising the increased vulnerability of young people in the digital environment.
- Criminal Offense to Outlaw Doxing: Doxing is the act of publishing private or identifying information about an individual on the internet, typically with malicious intent. Making it a criminal offence would mean that individuals engaging in doxing could face criminal charges and potential imprisonment. The Bill introduces maximum penalties of six and seven years prison time for offenders where a group is targeted based on race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin.
- Simplified international data sharing: The Government plans to identify countries and certification schemes that offer privacy protections comparable to Australia's, simplifying the process for organisations to share information internationally - a critical aspect of the digital economy without borders. This move will be a relief for private sector organisations that have previously grappled with the complexity of assessing the 'adequacy' of foreign privacy laws or creating contractual measures to compensate for it. However, foreign investors in Australia should be aware that the Foreign Investment Review Board's (FIRB) data conditions are still likely to be attached to how those investors hold data about Australians; particularly sensitive data or data about defence personnel.
- Streamlined information sharing in the case of an emergency or eligible data breach: The efficient exchange of information during emergencies or qualified data breaches can reduce the consequences of significant data breaches incidents. For instance, this system could alert financial institutions when identity documents are at risk, allowing them to implement increased surveillance and additional protective measures to shield clients from potential financial fraud.

What do the changes mean?

- Increased Compliance Obligations: With broader enforcement powers for the Information Commissioner and the introduction of a statutory tort for serious invasions of privacy, organisations handling personal information will need to ensure they have robust privacy practices in place. This includes securing personal information, obtaining clear consent for its use, and being transparent about data processing activities.
- Enhanced Transparency Requirements: The requirement for greater transparency around automated decision-making means organisations handling personal information will need to disclose more about their use of algorithms and AI in processing personal information. They may need to provide individuals with explanations of decisions made automatically, which could require adjustments to their systems and processes.
- Special Considerations for Children's Data: The additional protections for children's privacy will necessitate stricter controls over the collection, use, and sharing of data belonging to minors. This may involve implementing age verification mechanisms and obtaining parental consent where necessary.
- Legal Risks from Doxing: The criminalisation of doxing introduces a new legal risk, emphasising the importance of safeguarding personal information to prevent unauthorised disclosure that could harm individuals.
- Easier International Data Sharing: The mechanism to identify countries and certification schemes with privacy protections similar to Australia's will streamline the process for organisations to share information internationally. This reduces the burden of assessing foreign privacy regimes' adequacy and negotiating contractual safeguards, making

compliance easier and potentially opening up new markets. However, foreign investors subject to data conditions should check with the FIRB how those conditions will be impacted by these proposed data sharing arrangements.

- Streamlined information sharing during emergencies or eligible data breaches: This change would necessitate organisations handling personal information to adapt to new compliance requirements. It also offers the advantage of enhanced fraud prevention measures and the potential for increased trust and reputation protection by taking proactive personal information protection efforts.

Actions to consider now

Organisations operating in Australia, as well as global companies with Australian customers, will need to closely monitor these developments and prepare to comply with the new requirements. In light of reforms proposed in the Bill, affected parties will want to consider actions such as the below:

- Become compliant with the current requirements of the Privacy Act now – the Information Commissioner will have more funding and powers to investigate breaches and enforce the law.
- Undertake a privacy compliance gap assessment and get support from a privacy subject matter expert to recommend remediation actions and build out a roadmap toward compliance. This will include having strong privacy governance and practices in place and practical policies and processes to support organisations to implement compliance with the Privacy Act into business as usual practices.
- Pay attention to data breach response plans, data retention and third-party supplier management – these issues are common areas of struggle.
- An organisation's employees and the third parties it shares personal information with are its greatest sources of privacy risk. Put mandatory privacy training in place for all employees and create a strong vendor vetting, onboarding and management framework.
- Take special precautions when implementing new technologies or processing activities like the use of AI. Undertaking a Privacy Impact Assessment is best practice.
- Pay attention to international disclosures of personal information – have appropriate terms in place with third parties to ensure personal information is protected. If you are subject to FIRB data conditions, make sure that your privacy governance framework and contracting arrangements support this compliance.
- Know that international privacy laws (like the General Data Protection Regulation) have extraterritorial application and can affect Australian-based organisations.
- Be aware that law reform and guidance is being issued by government and regulatory authorities in relation to other key digital issues like cybersecurity, the use of AI and combating the spread of mis- and dis-information online.
- Keep in mind that further changes to the Privacy Act are anticipated.

What next?

- The Bill is expected to undergo Parliamentary Committee review and will likely be made into law in 2025.
- Expect a second tranche of even more substantial changes to be published in the near future.
- The second tranche is not the only piece of legislation that the Government is considering. We are expecting to see more for AI and data. There may also be further legislative developments in the States – such as South Australia for age verification of children on social media platforms and AI in New South Wales.

How EY can help

We can assist you with:

- Undertaking privacy compliance gap assessments
- Compliance remediation action plans
- Implementing recommendations across the full spectrum of privacy compliance
- Conducting Privacy Impact Assessments (PIAs) for new technologies and high-risk processing activities
- Mapping your data flows
- Data breach response plans and processes
- Training your employees
- Creating vendor onboarding processes that include privacy compliance
- Understanding the application of privacy and data protection laws

For more information please contact your usual EY adviser or any of the below:

Sydney:

Amber Cerny
Tel: +61 2 8295 6307
amber.cerny@au.ey.com

Melbourne:

Lucy Hannah
Tel: +61 2 8295 6467
lucy.hannah@au.ey.com

New Zealand:

Emma Maconick
Tel: +64 9 348 6604
emma.maconick@nz.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

About EYs Tax services
Your business will only succeed if you build it on a strong foundation and grow it in a sustainable way. At EY, we believe that managing your tax obligations responsibly and proactively can make a critical difference. Our global teams of talented people bring you technical knowledge, business experience and consistency, all built on our unwavering commitment to quality service – wherever you are and whatever tax services you need.

We create highly networked teams that can advise on planning, compliance and reporting and help you maintain constructive tax authority relationships – wherever you operate. Our technical networks across the globe can work with you to reduce inefficiencies, mitigate risk and improve opportunity. Our 50,000 tax professionals, in more than 150 countries, are committed to giving you the quality, consistency and customization you need to support your tax function.

For more information, please visit www.ey.com/au

SCORE NO: 007851-24-AUNZ
ED None