PRIVACY REVIEW 2023/2024

LANDER & ROGERS

Guide

INTRODUCTION

The last 12 months have been a big year for privacy. The Australian Government introduced the first tranche of reforms to implement a number of the recommendations from the Attorney-General's Department's Privacy Act Review Report, with further reforms to follow; and the Office of the Australian Information Commissioner signalled an ongoing focus on regulatory action where it identifies non-compliance.

In this update, we summarise key incidents and developments from the last year and highlight areas to watch in coming months.

We will continue to monitor developments throughout 2024 and beyond with keen interest.

In this guide

- Australian Government responds to Privacy Act Review
- AAT case: *HYYL and Privacy Commissioner* [2023] AATA 2961 (13 September 2023)
- ASX updates guidance on continuous disclosure obligations for ASX-listed companies following a data breach
- ACCC's Digital Platform Services Inquiry - 8th Interim Report
- OAIC Notifiable Data Breaches Report: July to December 2023
- Digital ID Act Begins on 1 December 2024
- OAIC Notifiable Data Breaches Report: January to June 2024
- The privacy outlook in 2024 and beyond

Timeline of key events

13 September 2023

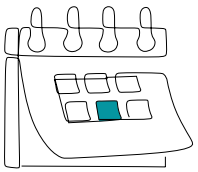
Administrative Appeals Tribunal (AAT) publishes *HYYL and Privacy Commissioner* [2023] AATA 2961.

28 September 2023

Australian Government releases its response to the Privacy Act Review Report.

27 November 2023

Attorney-General the Hon Mark Dreyfus KC MP announces the appointment of Carly Kind as Privacy Commissioner, reinstating the standalone position.



22 February 2024

The OAIC releases its Notifiable Data Breaches Report: July to December 2023.

21 May 2024

The Australian Competition & Consumer Commission (ACCC) releases its eighth interim report for the Digital Platform Services Inquiry, shining a spotlight on the supply of data products and services by data firms in Australia.

27 May 2024

The ASX releases its updated guidance on data breach continuous disclosure obligations for ASX-listed companies.

12 September 2024

Privacy and Other Legislation Amendment Bill 2024 introduced into Federal Parliament.

16 September 2024

OAIC releases its Notifiable Data Breaches Report: January to June 2024.

AUSTRALIAN GOVERNMENT RESPONDS TO PRIVACY ACT REVIEW

On 28 September 2023 the Australian Government released its response to the Privacy Act Review Report.

The much-anticipated Privacy Act Review Report was published in February 2023 and contained 116 proposals aimed at strengthening the *Privacy Act 1988* (Cth) following a number of high-profile data breaches and privacy incidents impacting Australian businesses and citizens.

The Australian Government "agreed" to 38 proposals, "agreed in principle" to 68 proposals and "noted" 10 proposals.

This response signalled a clear intention to continue to strengthen privacy laws in Australia.

First tranche of privacy reforms released

On 12 September 2024, the Attorney-General introduced the *Privacy and Other Legislation Amendment Bill 2024* (**Amending Bill**) into Federal Parliament. The Amending Bill represents the first tranche of privacy reforms to implement the recommendations from the Privacy Act Review Report and other reforms (view our insight for further information about the Amending Bill).

The Amending Bill addresses a number of the proposals the government "agreed" to in its response:

- **Proposals 3.1 and 3.2:** amend objects of the Privacy Act to clarify that the Act is about the protection of personal information and to recognise the public interest in protecting privacy.
- **Proposals 5.1 and 5.2:** grant power to the Information Commissioner to make an APP code or issue a temporary APP code where the Attorney-General has directed or approved that a code should be made.
- **Proposal 16.5:** introduce a Children's Online Privacy Code that applies to online services that are likely to be accessed by children.
- **Proposals 19.1-19.3:** privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights. High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights to be included in the Act. Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.
- **Proposal 21.1:** amend APP 11.1 to state that "reasonable steps" include technical and organisational measures.
- **Proposal 23.2:** introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).
- **Proposal 25.1:** create tiers of civil penalty provisions to allow for better targeted regulatory responses.
- **Proposal 25.2:** amend section 13G of the Act to remove the word "repeated" and clarify the meaning of "serious".
- **Proposal 25.5:** amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss following an Information Commissioner's investigation.

The Australian Government will conduct targeted consultations in respect of a number of the more significant proposals relating to removing the small business exemption and the employee records exemption.

It is evident the government is committed to consulting with relevant stakeholders to properly understand the impact of removing the exemptions. However, we anticipate it is only a matter of time until the small business exemption and employee records exemptions are removed from the Privacy Act.

Key takeaways

While we wait for the Amending Bill to pass through Parliament, organisations should continue to review and uplift their privacy compliance activities to place themselves in the best possible position to respond and adapt to the strengthening of privacy laws in Australia.

AAT RULES DATA BREACH CLASS MEMBERS MUST PROVE ACTUAL LOSS AND DAMAGE

Over the past 12 months we have witnessed the largest data breaches in Australia's history, which have brought into sharp focus the risk of data breach class actions and their financial consequences.

The amount of compensation payable to affected individuals must be considered as part of an overall assessment of the likely financial loss an organisation may suffer as the result of a data breach.

In the case of *HYYL and Privacy Commissioner* [2023] AATA 2961 Justice Melissa Perry, sitting in the Administrative Appeals Tribunal of Australia (**AAT**), considered the question of compensation eligibility and assessment of compensation under the *Privacy Act 1988* (Cth).

Background to AAT case

The data breach

On 10 February 2014 the Department of Immigration and Border Protection (**Department**) published on its website a Microsoft Word document dated 31 January 2014 and titled "The Immigration Detention and Community Statistics Summary" (**Detention Report**). The report included an embedded Microsoft Excel spreadsheet that was used to generate the statistics in the Detention Report. The spreadsheet included the personal information of 9,258 individuals who were in immigration detention on 31 January 2014. This raw data was accessible through the Detention Report. The Detention Report was publicly accessible on the website for approximately eight days and on the Internet Archive for 16 days.

OAIC own motion investigation

On 21 February 2014 the Australian Information Commissioner (**AIC**) opened an own motion investigation into the Department and considered the Department's security practices and whether there was an unauthorised disclosure of personal information under the Privacy Act. It found the Department breached IPP 4(a) by failing to put in place reasonable security safeguards to protect personal information, and IPP 11 as the publication of the embedded spreadsheet constituted an unauthorised disclosure of personal information.

Further information about the investigation can be found on the OAIC website.

AIC determination

Separately, the AIC received and considered a representative complaint made by one of the affected individuals under section 36 of the Privacy Act. Under section 52 of the Act, the AIC may award compensation to affected individuals for loss or damage suffered as a result of an interference with their privacy. The AIC determined (amongst other things) that certain affected individuals who did not opt out of the representative proceedings were entitled to be paid compensation for loss or damage arising from the data breach, provided those individuals established that they suffered loss or damage by reason of the Department's interference with their privacy. The amount of compensation payable would be determined in accordance with the process specified in the AIC's determination.

Further information about the AIC's determination can be found on the AustLii website.

AAT decision

The applicants to the AAT proceedings, HYYL and WP, both sought to set aside the AIC's determination. In particular, the applicants argued the quantum of compensation determined by the AIC was below the quantum that ought to be awarded to the affected individuals in the circumstances of this case.

On the question of compensation, the AAT determined:

- participating class members of the representative complaint **must provide evidence** to substantiate claims of loss or damage they suffered as a result of the data breach before any entitlement to compensation under section 52 of the Privacy Act can arise
- magnitude of harm and quantum for non-economic loss should be assessed against a set number of categories of non-economic loss and fixed amounts. Damages must be compensatory and restrained under the Privacy Act.

Key takeaways

Organisations will be relieved that affected individuals must substantiate compensation claims for loss or damage they suffer as a result of a data breach under the Privacy Act. Given it can be challenging for affected individuals to evidence actual loss or damage at the time of a data breach, it will be difficult for affected individuals to successfully seek compensation under the existing Privacy Act regime.

This case is significant as it is the first AAT case to consider the issue of compensation in a representative proceeding under the Privacy Act. While the AAT's decision is not binding on the AIC, it provides a useful reference point that is likely to be considered by the AIC when assessing non-economic loss or damage in future representative complaints.

The AAT decision *HYYL and Privacy Commissioner* [2023] AATA 2961 can be found on the AustLii website.

ASX UPDATES GUIDANCE

ASX updates guidance on continuous disclosure obligations for ASX-listed companies following a data breach

On 27 May 2024, the ASX updated the 'Listing Rules Guidance Note 8 Continuous Disclosure' (latest version here, mark-up version here) (**Guidance Note**) to include a hypothetical data breach scenario. While the continuous disclosure obligations for ASX-listed entities have not changed, the update sets out the ASX's expectations as to the content and timing of disclosure to the ASX following a cyber security incident. The example scenario illustrates how the ASX would apply the ASX Listing Rule 3.1 and ASX Listing Rule 3.1A to a data breach scenario.

Continuous disclosure regime

Under ASX Listing Rule 3.1, ASX-listed entities must comply with the general rule of continuous disclosure:

"Once an entity is or becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities, the entity must immediately tell ASX that information."

ASX Listing Rule 3.1 would not apply if the requirements for the exemption listed in ASX Listing Rule 3.1A are satisfied:

"3.1A.1 Any one or more of the following situations applies:

- *it would be a breach of a law to disclose the information;*
- *the information concerns an incomplete proposal or negotiation;*
- *the information comprises matters of supposition or is insufficiently definite to warrant disclosure;*
- *the information is generated for the internal management purposes of the entity; or*
- *the information is a trade secret; and*

3.1A.2 The information is confidential and ASX has not formed the view that the information has ceased to be confidential; and

3.1A.3 A reasonable person would not expect the information to be disclosed."

Application of the ASX Listing Rules: ASX data breach example

When disclosure is not expected

While the data breach scenario specifically concerns an entity that holds a "significant amount of personal information about its customers", including "sensitive information" and "credit card details", the guidance is still relevant for all ASX-listed entities that may experience a data breach.

The ASX emphasises that, when an entity discovers a breach of its systems or information, the extent of the data breach may at first be unclear. Accordingly, disclosure may not be required at this stage and forensic experts may need to be engaged to conduct investigations. However, ASX's expectation is that any forensic work or investigation is conducted with "urgency".

With limited information, an entity is unlikely to be able to determine the potential adverse consequences and whether the breach is material to the price or value of its securities. Listing Rule 3.1A would likely be satisfied in these circumstances as the matter "is insufficiently definite to warrant disclosure".

Even where a ransom demand is made and the entity confidentially engages with regulators, or a forensic expert confirms that a data breach has occurred, disclosure may not be required if the type of information accessed, or the extent of the breach, is unclear. This is because the consequences of the breach are still uncertain, and it cannot be determined at that point in time if it is materially price sensitive.

When is disclosure required?

The updated Guidance Note describes the following circumstances where disclosure is required:

- The breach ceases to be confidential - such as when an entity intends to notify affected individuals, there are rumours or media commentary regarding the breach, or there is notification that an article on the breach will be published;
- The ASX requires the entity to make an announcement where it detects abnormal trading in the entity's securities or considers there is or likely to be a false market in the entity's securities (whether or not the entity believes the breach is materially price sensitive); or
- There is likely to be a material effect on the price or value of the entity's securities from the breach, such as where unencrypted personal information for a large number of customers has been exfiltrated from the entity's systems by a threat actor.

Continuous disclosure

Further disclosures may be necessary where:

- there is a new development that a reasonable person would expect to significantly impact the price or value of the entity's securities; for example, if personal information is subsequently released onto the dark web by cyber criminals; or
- a class action is served, or information about a potential legal claim becomes materially price sensitive.

In each case, the disclosures are predicated on whether they relate to materially price sensitive information.

PRIVACY REVIEW 2023-2024

Key takeaways

While the continuous disclosure obligation will largely differ depending on each case, listed entities should consider the following in the event of a data breach.

Investigation

Conduct all necessary forensic investigations with urgency as soon as a potential data breach is discovered.

Notify regulators

If a decision is made to notify regulators of the data breach, this ought to be done on a confidential basis while disclosure is not required and information about the data breach remains confidential.

Access legal advice

Engage legal representation, as appropriate, to assist with establishing privilege and crisis management.

Notify the OAIC

Formally notify the Office of the Australian Information Commissioner (OAIC) of the data breach if it satisfies the notification criteria and in accordance with the requirements of the *Privacy Act 1988* (Cth).

Prepare an announcement

During investigations, prepare a draft announcement that may be rapidly released if disclosure is required, including initial details (to be updated as the entity becomes aware) including:

- what has occurred and details of the breach
- material impacts on the entity's operations or financial position
- action being taken in response to the breach
- when an update will be issued to the market
- to the extent that it is known or relevant:
  - the type of data potentially accessed
  - whether the data has been exfiltrated
  - the number of customers or accounts impacted
  - arrangements for notifying impacted customers
  - whether data was accessed through the entity's systems or a third-party system
  - whether the incident is continuing
  - if the breach is still being investigated and whether the extent of the breach or its impacts are known.

Trading hold

If the data breach becomes disclosable in accordance with the Listing Rules, but the organisation is not able to make the disclosure with sufficient certainty, engage with the ASX and request a trading hold (for no more than two days) or voluntary suspension from ASX. While these are granted by the ASX in its discretion, they provide extra time to prepare and/or update an announcement to be released promptly to the market.

Further disclosures

Make further disclosures as necessary, particularly in relation to all materially price sensitive information as and when the organisation becomes aware of such information.

ACCC'S DIGITAL PLATFORM SERVICES INQUIRY

Eighth interim report

Background

In 2020 the Federal Government directed the Australian Competition & Consumer Commission (**ACCC**) to conduct a five-year inquiry into the markets for the supply of digital platform services (**DPS Inquiry**). "Digital platform services" include internet search engines, social media, private messaging platforms, digital content aggregation platforms and electronic marketplace services, as well as media referral services provided in the course of delivering any of the aforementioned services.

The DPS Inquiry looks to examine the behaviours and practices of suppliers of digital platform services (including the nature of services offered, and whether suppliers' privacy and data collection, management and disclosure practices may result in harm to consumers) as well as the operation of the *Competition and Consumer Act 2010* (Cth) (**Competition & Consumer Act**) with respect to regulating digital platform services markets. The DPS Inquiry has made a number of market observations to date. It has also highlighted the potential risks to consumers and competition posed by the expanding digital platform services ecosystem, and recommended reforms that would impact both businesses and consumers.

The eighth interim report for the DPS Inquiry considers potential competition and consumer issues in the supply of data products and services by "data firms" in Australia, specifically with respect to how information is collected and used by such firms. "Data firms" are businesses that provide data collection, storage, supply, processing and analysis services, but do not generally have a direct relationship with the relevant original individual or entity from which the data was collected.

Whilst the report does not strictly address matters from the perspective of the *Privacy Act 1988* (Cth), it does consider practices of data firms with respect to "consumer data" (i.e. "personal or other information on persons" generally).

Market observations by the ACCC

The ACCC acknowledged in the report that data firms offer data products and services that "play an important role in the economy and have a range of benefits for businesses that use them". Additionally, the ACCC noted that public sector entities also utilise data products and services. These products and services can provide entities with new or enriched data and analytics, which may assist in functions such as marketing, advertising, risk management and general optimisation. The report noted that nearly "every industry in Australia uses data products and services from data firms".

The ACCC observed that data firms collect a wide range of sensitive or personal data from various sources. This includes by way of access to publicly available data and statutory data-sharing schemes, as well as the purchase and licensing of data from other organisations. Information collected by data firms includes:

- identifying information
- demographic data
- financial and transactional data
- location data
- preferences
- medical information
- criminal history
- biometric data.

The report observed that data products and services are "highly customisable" as data firms may provide services on "pay per use", subscription/licensing, "no-monetary-cost", or reciprocal arrangements. The report also observed that data firms "sometimes" (i.e. not in all instances) provide products and services with conditions pertaining to the use and security of underlying data.

Concerns identified by the ACCC

Areas of concern identified by the ACCC in relation to harmful practices in the data product and services industry include:

- the likelihood of consumers providing "uninformed consent" when agreeing to terms and conditions (including any incorporated privacy policies) to access goods and services
- consumers' limited practical ability to exercise their rights under Australian privacy law to access and correct their personal information, and
- the potential for vulnerable consumers to be identified and targeted.

Giving rise to the ACCC's concerns were its observations that:

- approximately 74% of consumers are uncomfortable with the notion of their personal information being shared or sold
- the terms included in privacy policies are often vague and broad
- there is a general lack of transparency with respect to access or control of consumer data by third parties
- many consumers are unaware of the practices of data firms and other entities with respect to collecting, using and disclosing their data

PRIVACY REVIEW 2023-2024

- it would take approximately 46 hours per month for a person to read every privacy policy they encountered
- many consumers do not engage with reading privacy policies
- consumers are generally required to accept a provider's standard terms and conditions (including any incorporated privacy policy) to utilise a product or service.

Reforms recommended by the ACCC

The report builds upon the regulatory reform recommendations of the ACCC's fifth interim report. Key recommendations from the fifth interim report include the introduction of economy-wide measures to protect consumers, including a general prohibition against unfair trading practices; and a power enabling the ACCC to implement mandatory codes of conduct for specific services provided by designated digital platforms, to address relevant issues that may arise.

Key takeaways

Organisations that collect or use consumer data should take note of the concerns raised by the ACCC in the DPS Inquiry. These findings may give rise to greater regulatory and policy scrutiny once the DPS Inquiry is complete.

Organisations should pay specific attention to whether their standard terms and conditions, and privacy policies, present risks arising from lack of transparency, unfair contract terms, or misleading and deceptive conduct.

NOTIFIABLE DATA BREACHES REPORT JULY TO DECEMBER 2023

On 22 February 2024 the Office of the Australian Information Commissioner (OAIC) published its Notifiable Data Breaches Report for the period of July to December 2023.

Key findings

In the July to December 2023 reporting period:

- 483 separate breaches were raised through primary notifications, representing a 19% increase over the preceding period
- the health and finance sectors were most affected by reported data breaches, with 104 breaches reported in health (22%) and 49 breaches reported in finance (10%)
- the leading cause of reported data breaches remained criminal or malicious attacks, representing 67% of all notifications
- most breaches (84%) that affected more than 5,000 people were caused by criminal or malicious attacks involving cyber incidents
- there was a significant increase in secondary notifications, totalling 121 in this reporting period compared to 29 in the January to June 2023 period. Secondary notifications may relate to a primary notification received in a prior reporting period.

Overview

A total of 483 data breaches were reported, marking a significant increase from the previous reporting period. The most breached information types included contact information, financial details, identity information, and health records.

Breaches by category

Malicious or criminal attacks (including cyber incidents such as phishing or stolen credentials, social engineering, rogue employees, and theft of data) were the most significant source of breaches, marking 67% of all notifications. A quarter of all incidents were caused by stolen credentials alone.

Human errors were the next largest cause of breaches, at some 30% of all notifications. The apportionment of causes drops steeply beyond these categories, with only 4% of breaches caused by the next significant contributor, systems faults. Notwithstanding the cause of the breach, the OAIC was generally (72% of the time) notified within 30 days.

Secondary breaches

The report also noted a substantial increase in duplicate notifications in relation to the same incident ("secondary notifications"). Most of these breaches involved a cloud or software provider exposing their client's personal information.

Large breaches

Cyber incidents remained the leading cause of data breaches, affecting over 5,000 Australians and totalling 22 of the 26 breaches in this category. These large breaches were generally caused by stolen credentials (9), ransomware (8) and hacking (4), and affected 56,279 individuals on average.

Industry impacts

Overall, health service providers reported the highest number of breaches (22%), followed by finance (10%), insurance (9%), retail (8%) and the Australian Government (8%). However, breaches occurred across various sectors, reflecting the widespread vulnerability of organisations to data security threats in any industry or sector.

Key risks

It is evident that online threat actors are becoming increasingly prevalent, and threats more sophisticated, given the high rate of cyber incidents in the latter half of 2023. As these incidents tend to disproportionately affect large numbers of individuals, they expose organisations that suffer a breach to significant consequences. Cyber incidents pose a major challenge to data security efforts, requiring organisations to implement robust cyber security measures and incident response plans and to ensure that they continue to evolve.

One emerging risk identified in the report includes the outsourcing of data handling to third-party providers. The OAIC recommends that entities review the security and operational controls of third-party providers to ensure they limit the potential for customers' personal information to be compromised. Any service agreements should also address the handling of personal information, including data retention periods, processes for destroying data, and suppliers' data breach response requirements, such as contractually binding reporting obligations.

DIGITAL ID ACT BEGINS ON 1 DECEMBER 2024

Introduction

The *Digital ID Act 2024* (Cth) (**Digital ID Act**), anticipated to commence on 1 December 2024, will revolutionise identity verification services in Australia by establishing a nationwide Digital ID system comprising four key elements.

1. Establishing the Australian Government Digital ID System.
2. Expanding the existing voluntary Digital ID accreditation scheme.
3. Imposing privacy and security obligations on accredited entities in addition to the *Privacy Act 1988* (Cth) (**Privacy Act**).
4. Appointing a Digital ID Regulator (initially the Australian Competition & Consumer Commission) to accredit and approve Digital ID system participants under the Digital ID Act, and to enforce compliance with non-privacy aspects of the Act. The Office of the Australian Information Commissioner (**OAIC**) will be the regulator in relation to the privacy aspects of the Act.

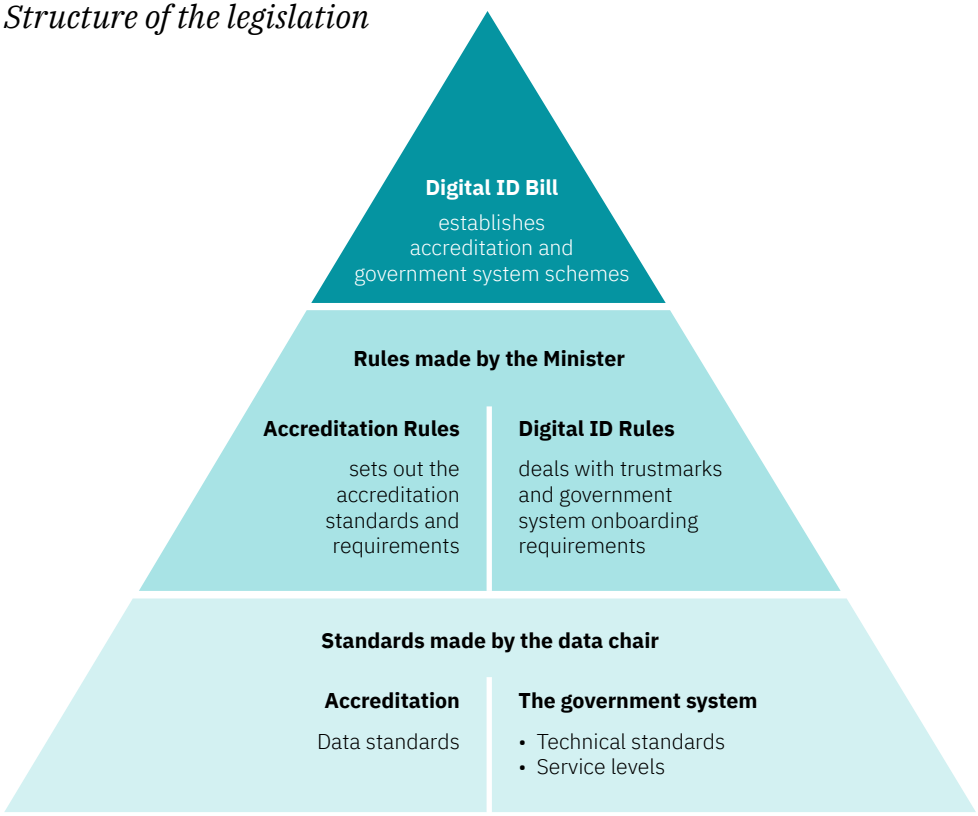
Participating organisations will be able to rely on a Digital ID to verify a consumer's identity rapidly and securely through the Digital ID system. "Accredited entities" will provide Digital ID services and "relying" entities will be able to provide services to a consumer by relying on the consumer's Digital ID. It is envisioned that, under this system, a consumer will only need to disclose key personal information to a select few accredited entities that adhere to strict data security standards.

In addition to the Act, there are Digital ID Rules and Accreditation Rules (collectively, the **Rules**) which will specify the requirements of the Digital ID system in greater detail. The draft Rules have been published for public comment.

Further, under the Digital ID Act, a "Digital ID Data Standards Chair" appointed by the Minister for Finance may make data standards that set out the technical integration requirements for participating entities, and technical data or design standards regarding accredited entities. The proposed data standards have also been issued for public comment.

The Australian Government has published the following infographic setting out the relationship between the Digital ID Act and its associated Rules and Data Standards.

Structure of the legislation



The Digital ID legislation is a package of legislative instruments governing the Accreditation Scheme and the Australian Governemet Digital ID system.

PRIVACY REVIEW 2023-2024

Australian Government Digital ID System

The Australian Government Digital ID System (**AGDIS**) is an existing system that includes the myGov and myGovID services. Initially targeted at Commonwealth Government non-corporate entities, the AGDIS will eventually be expanded to non-government entities under the Digital ID Act.

With the commencement of the Digital ID Act, approval to participate in the AGDIS will require entities to receive accreditation and meet further requirements, including the Digital ID data standards and conditions imposed by the Regulator or the Rules. The accredited entity must also demonstrate that its service is interoperable with the broader AGDIS ecosystem.

Relying parties do not need accreditation to participate in the AGDIS, but must be approved by the Regulator before participating. To receive approval, entities must conduct interoperability testing, fraud management, business continuity and cyber security incident risk assessments.

Accreditation

The Digital ID Act's accreditation scheme is a significant component of the broader system. Expanding upon the existing unlegislated Trusted Digital Identity Framework (which supports MyGov), the Digital ID Act will establish three types of accredited entities:

1. **Identity service providers**, who will assist a user with creating or maintaining a Digital ID and deal with identity authentication;
2. **Attribute service providers**, who are responsible for overseeing changeable "attributes" unrelated to identity that are linked to a person's Digital ID; and
3. **Identity exchange bodies**, which will facilitate the Digital ID system by shifting information between identity service providers, attribute service providers and relying parties.

Entities seeking accreditation must comply with stringent requirements, including conducting initial and annual privacy impact assessments, assurance assessments and systems testing. Only Australian companies, Australian government organisations and foreign companies registered with ASIC can seek accreditation.

Accredited entities will be eligible to participate in the AGDIS if approved by the Regulator and will be able to use a "trust mark" to certify their accreditation with consumers.

The Regulator retains significant discretionary power over an entity's accreditation, and can revoke or suspend the accreditation if certain criteria are satisfied. These include a breach of the Digital ID Act or Accreditation Rules, involvement in a cyber security incident, if the national interest supports the removal of the accreditation, or if it is no longer appropriate for the entity to hold such accreditation.

Privacy

The OAIC will be responsible for overseeing the Privacy Act aspects of the AGDIS, which will include:

1. notifying any "cyber security incident" to the OAIC, including unauthorised attempts to cause a data breach;
2. notifying individuals of risks in the Digital ID system or cyber incidents;
3. extending protections to "attributes" not covered by the Privacy Act, including personal data even if not directly related to an identifiable individual; and
4. complying with the Australian Privacy Principles, which include restrictions on collecting, distributing, and using certain personal data.

Sensitive personal data will be subject to particularly strong protections. Entities must not intentionally collect data pertaining to attributes such as racial or ethnic origins, political opinions, membership of a political association, religious or philosophical beliefs, or sexual orientation or practices.

Biometric data will be restricted to collection for identity verification and authentication purposes, and there will be obligations to destroy this data within set time limits.

Impacts and next steps

A secure and strong Digital ID network is essential to safeguarding Australia's future digital economy. The Digital ID Act will be the platform on which this Digital ID network is built, establishing a system that reduces identity theft, fosters privacy, and increases business efficiency by making Digital IDs safe, reliable, and simple.

While the application of the Digital ID Act will initially be limited to government agencies, forward-thinking organisations - particularly banks, credit providers and payment service providers - should prepare for its expansion to the private sector.

Most companies will only interact with the Digital ID Act as a relying party when they seek to verify a customer using their Digital ID. These businesses will need to review their interoperability testing, fraud management, business continuity and cyber security incident risk assessment before seeking approval to participate in the Digital ID system.

Despite these additional compliance requirements, the benefits of Digital IDs may be significant, allowing these businesses to expend fewer resources by performing faster ID checks of a higher standard, while limiting the personal information held in their own systems. Reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) will find these benefits particularly relevant when conducting know-your-customer (KYC) checks.

Organisations seeking deeper involvement in the Digital ID ecosystem, either as providers or intermediaries for digital identity services, will need to closely review their business models to determine their obligations and the steps they will need to undertake to seek accreditation.

From a public interest perspective, it is anticipated the Digital ID system will streamline costly in-person or over-the-phone identity verification for government, financial services and health sectors. $288 million has been allocated in the 2024-2025 federal budget to support the new Digital ID system.

By reducing the number of entities holding personal information, and by requiring strict cyber security standards, the Digital ID system will limit the risks and impacts of data breaches.

NOTIFIABLE DATA BREACHES REPORT: JANUARY TO JUNE 2024

On 15 September 2024, the Office of the Australian Information Commissioner (**OAIC**) released its Notifiable Data Breaches Report for the period between January to June 2024.

Report summary

During this period the OAIC reports:

- it received 527 data breach notifications, an increase of 9% compared to the previous six months;
- cyber security incidents continue to be a prevalent cause of data breaches;
- 63% of data breaches affected 100 or fewer people; and
- one reported incident affected over 10 million Australians, representing the second breach recorded to affect more than 10 million Australians and the highest number of individuals affected by a breach since the Notifiable Data Breaches Scheme came into effect.

The main sources of data breach incidents continue to be system fault, human error, and malicious or criminal attack. This provides organisations with a useful reference point to assist with prioritising risk mitigation and identifying where to proactively invest resources into cyber security and privacy compliance.

Key themes and issues

The report highlights a number of themes and issues the OAIC has observed from the notifications it has received, which presents organisations with a useful list of risks and issues to address.

Mitigating cyber threats

The OAIC expects entities to have appropriate and proactive measures in place to mitigate cyber threats and protect the personal information they hold.

Addressing the human factor

Individuals remain a significant threat to an entity's privacy compliance. Entities need to minimise the risk of individuals intentionally or inadvertently contributing to the occurrence of data breaches.

Being proactive in communicating the occurrence of a breach

Entities should not rely on assumptions and should weigh in favour of notifying the OAIC and affected individuals when a breach occurs.

Extended supply chain risks

Entities that outsource the handling of personal information can reduce the impact of a data breach in the supply chain by implementing a robust supplier risk management framework.

Misconfiguration of cloud-based data holdings

Entities need to be aware that there is a shared responsibility for the security of data in the cloud.

Data breaches in the Australian Government

Government agencies, especially those with service delivery functions, need to build community trust in their ability to protect the security of individuals' personal information.

Key takeaways

The OAIC has made it clear that privacy should not be an afterthought, and organisations are expected to comply with their privacy obligations. With the first tranche of privacy reforms progressing through Parliament - which includes the introduction of a tiered penalty regime to provide the OAIC with powers to issue infringement notices for lower level breaches - we encourage organisations to prioritise privacy compliance and continuous improvement.

THE PRIVACY OUTLOOK IN 2024 AND BEYOND

In the last 12 months, privacy reform and the threat of data breaches have been front of mind for organisations as the regulatory and threat landscape has continued to evolve in complexity and risk.

The Privacy Commissioner commenced a number of civil penalty proceedings and investigations into high-profile data breaches and the privacy practices of well-known companies. The Office of the Australian Information Commissioner (**OAIC**) has made it clear that it is prepared to start civil penalty proceedings against organisations alleged to have breached Australian Privacy Principle 11 - the failure to take reasonable steps to protect personal information.

With the first tranche of privacy reforms underway (the *Privacy and Other Legislation Amendment Bill 2024* was introduced in Federal Parliament on 12 September 2024), now is the time for organisations to review their current privacy practices and invest in measures to ensure ongoing compliance with the Privacy Act, strengthen information security protections, and safeguard controls of digital assets. This includes:

- assessing current data holdings to understand where all personal information is stored and whether the information is adequately protected;
- reviewing data retention and destruction policies and procedures to mitigate the risk of over-collection and storage of personal information;
- reviewing privacy policies, procedures and data breach response plans to ensure these documents are up to date and remain fit for purpose;
- conducting regular staff privacy training and awareness activities; and
- convening a subcommittee to start preparing for the anticipated privacy reforms.

Privacy remains high on the agenda as:

- emerging technology, such as artificial intelligence (**AI**), raises fundamental questions about the safeguarding of privacy and protection of personal information (and, in that regard, the Federal Government has only recently released its Voluntary AI Safety Standard and is currently debating whether to introduce new legislation on AI);
- supply chains become more complex and data storage (including personal information) is increasingly outsourced to third parties; and
- the frequency of cyber attacks continues to rise each year.

Lander & Rogers' Digital Economy practice will continue to monitor the evolution of the privacy landscape and share insights on privacy reform developments as they occur.

CONTACTS

Editor

Keely O'Dowd

Contributors

Kenneth Leung
Michelle Zhu
Menake De Silva
With thanks to **Ryann Wong** and **Samara Jones** for their contribution to this guide

Key contacts

Matthew McMillan
Partner
Corporate

D +61 2 8020 7787
E mmcmillan@landers.com.au

Keely O'Dowd
Special Counsel
Corporate

D +61 3 9269 9526
E kodowd@landers.com.au

Robert Neely
Consultant
Corporate

D +61 2 8020 7704
E rneely@landers.com.au

Edward Lyons
Senior Associate
Corporate

D +61 2 8020 7613
E elyons@landers.com.au

ABOUT US

Lander & Rogers is a leading independent Australian law firm, with over 650 people and over 100 partners and a leader in legal tech and innovation.

With offices in Sydney, Melbourne and Brisbane, Lander & Rogers has grown organically resulting in a highly cohesive firm focused on delivering the best law firm experience for our people, clients, and the communities in which we operate.

"We believe legal services involve more than just the law – practical, commercial advice and an exceptional client experience are equally important to our clients and to us", says Genevieve Collins, Chief Executive Partner.

Lander & Rogers advises corporate, government, and private clients in corporate transactions, insurance law, employment law, construction & infrastructure, digital & technology, commercial disputes and family & relationship law.

The firm is global in approach, working closely with a network of leading firms to provide advice to clients, both domestically and abroad. Lander & Rogers is also the exclusive Australian member of the world's leading independent network of law firms, TerraLex.

Brisbane

Level 11 Waterfront Place
1 Eagle Street
Brisbane QLD 4000

T +61 7 3456 5000
F +61 7 3456 5001

Melbourne

Level 15 Olderfleet
477 Collins Street
Melbourne VIC 3000

T +61 3 9269 9000
F +61 3 9269 9001

Sydney

Level 19 Angel Place
123 Pitt Street
Sydney NSW 2000

T +61 2 8020 7700
F +61 2 8020 7701

landers.com.au