White paper

Are you ready for the Privacy Act changes?

Key Takeaways

- **Stricter data protection laws:** The amendments to the Australian Privacy Act will impose more stringent regulations on how organisations handle personal data.
- **Enhanced consumer rights:** Consumers will have greater control over their personal data, including easier access, corrections, and the right to request deletion.
- **Mandatory data retention periods:** New changes to Privacy Principle 11 introduce maximum and minimum data retention periods for personal information.
- **Increased penalties for non-compliance:** Fines for failing to meet the new privacy requirements will be significantly higher, reaching millions of dollars.
- **Immediate action required:** Organisations should start preparing now by following Iron Mountain's information transformation model of Discover, Unify, Govern, Automate, Unlock, and Maintain.
- **Operational benefits of compliance:** Beyond mitigating privacy risks, complying with the Privacy Act's requirements can unlock operational efficiencies and improve data utilisation, opening up new revenue opportunities.

What the new Privacy Act means for Australian organisations

Impending changes to the Australian Privacy Act will have far-reaching consequences for many organisations, with new tiered penalties introduced in addition to the existing fines of greater than $50 million for serious or repeated failures, even for small/medium sized businesses.

These sanctions are on top of the damage that can be done to business operations and brand value as a result of poor privacy protections. Optus for example was forced to set aside $140 million to cover the costs of its 2022 data breach, while the associated brand damage has been estimated at $1.5 billion. Over at Medibank, its breach led the Office of the Australian Information Commissioner (OAIC) to allege that the insurers seriously interfered with the privacy of 9.7 million Australians by failing to take reasonable steps to protect their personally identifiable information (PII) from misuse and unauthorised access or disclosure in breach of the Privacy Act.

The volume of incidents is also increasing, with the OAIC reporting that from January to June this year they received 527 data breach notifications – an increase of 9 per cent over the previous six months.

This combination of reputational damage, business impact, and potential penalties, along with the increasing likelihood of attack, should be enough to make any responsible business leader ask whether they are doing all they can do to ensure they are protecting the PII they're holding – especially those in the top five most at risk sectors of health services, the Australian Government, finance, education, and retail.

The proposed amendments come at a time when many organisations are still grappling with what it means to hold personal information in the digital age. Although traditionally this information resided within structured databases and records management systems, today personal information can be found in everything from email systems and spreadsheets to online form repositories and workplace collaboration applications.

> That means a larger number of staff members may now have responsibility for managing and protecting personal information, from records management professionals to IT managers and data officers.

What's changing in the Australian Privacy Act?

The Privacy and Other Legislation Amendment Bill 2024 includes 24 legislative proposals that data managers and record keepers will need to be aware of if they wish to keep their organisation compliant. However, these reforms represent only a quarter of the original recommendations to government, suggesting that further changes may lie in the near future.

Amongst these are changes to the definition of what constitutes personal information. For instance, personal information will now include information that 'relates to an individual', rather than just information about an individual. There are also new restrictions for how personal information can be used in marketing and changes to the scope of exemptions relating to employee records.

But perhaps the most profound changes relate to Privacy Principle 11 and come in the form of a requirement to implement maximum and minimum retention periods for different types of personal information, along with the mandated destruction of information when those retention periods have expired.

Should these proposed changes be enacted as amendments to the Privacy Act, they will require organisations to significantly strengthen their information management processes or risk investigation by the OAIC.

This means the best time to begin the process of understanding and preparing for these changes is now.

What you need to know: Practical steps for compliance

The path to compliance with the revised Privacy Act starts with understanding exactly what personal information your organisation holds.

Historically speaking, the responsibility for records management fell under the auspices of dedicated professionals, but over time the increasing digitisation of data has seen more and more of that responsibility fall to technical professionals and chief data officers.

With compliance requirements mounting, it is critical that whoever is now in charge of managing personal information has a skill set that crosses both realms.

These combined skills can be hard to find, however. For many organisations today, the challenge of PII management will require assistance from partners with expertise both in the traditional disciplines of records and information management as well as comprehensive capabilities when working in the world of data.

At Iron Mountain, we refer to this holistic information management process as the information transformation journey, and like most journeys, it involves multiple steps.

Discover what information your organisation holds

The first step in any information transformation is **Discover**, which describes the process of comprehensively understanding the information that your organisation holds.

A good starting point for any organisation is to know and understand the regulatory environment in which it operates, and therefore what information it needs to manage and govern so that it can operate in a compliant manner - regardless of the technology they are using to store and protect data. Understanding obligations also means understanding the various carve-outs that pertain to specific industries, such as when data needs to be retained for legal requirements including for compliance with anti-money laundering laws. In other words, what controls do you need to put in place to assure that you are compliant with your obligations?

This is a task that can be significantly harder than it sounds, given that the Act covers information that is stored both digitally and physically, including the many paper records that might be stored away in physical secondary storage or archives. Personal information can also include photographs, thanks to its definition extending to 'any evidence of business activity'.

The Privacy Act also makes no distinction regarding the digital systems (including line of business applications and databases) that personal information might be stored in. This means that data professionals and records managers will need to consider not only their structured records management systems and databases, but also ad hoc or unstructured formats such as spreadsheets, documents or even information stored within email systems.

A further warning for some regulated organisations is that failure to manage PII correctly could see them lose their licence to operate. This is specifically true for financial services organisations, where APRA's CPS 234 information security law makes specific demands for how organisations should maintain information security systems and practices that are appropriate for the threats they face, including maintaining a comprehensive inventory of all relevant data, processes, systems, and controls. Complying with the Privacy Act may also require some organisations to separate out PII from other records they might hold. For instance, if personal information has been used to establish a person's identity during a sign-up process, this information may need to be destroyed after a certain period, even though the non-PII elements of the record may be needed for other business reporting needs.

It is this level of nuance that will present a significant challenge to those professionals who are responsible for records and information management, and all these requirements make Discover one of the most important steps in the information maturity journey.

After all, it is impossible to ensure compliance with a law when you can't actually identify all of the assets it applies to.

Bring unity to records management

Once an organisation has gone through the Discover process it can move on to the second stage, which we call **Unify**. Unify describes the implementation of a comprehensive information management program that records the location of information and classifies its type, while also providing instructions for its management. By providing a unified picture of PII, it becomes much easier to then manage that data in ways that ensure the organisation remains compliant with the revised Act.

A critical outcome of the Unify stage is to deliver an understanding of the age of personal information stored and the implementation of rules relating to the retention periods.

The tendency for personal information to reside in many locations across an organisation will lead many to adopt the approach of 'manage in place', which alleviates any need to bring data sources together in a centralised repository in favour of systems which enable data to be managed where it is.

The goal of Unify is more than just technology. It is about creating a unified asset strategy that gives clarity to the type and location of all information, including personal information stored, along with its status within the information retention lifecycle, all managed by a centralised interface.

An additional benefit from the Unify stage is to give data managers the opportunity to reduce the total amount of data their organisation holds. While traditional thinking has led some organisations to retain all data 'just in case', recent breaches have demonstrated that this practice is a liability when older, low-value data is hacked or stolen.

Understanding the nature of personal information being held allows greater consideration of the reasons as to why, and hence an opportunity to reduce the amount of data retained. This is beneficial in terms of reducing the potential exposure through a data breach, while also lowering the overall costs of data storage.

This assessment may be especially important for those organisations that are considering the use of personal information in the training of AI models.

Governance for all

The third step on this path to information maturity is **Govern**, which uses the knowledge gained during the Discover and Unify phases and ensures that PII is managed in accordance with the revised Privacy Principles.

This serves to provide the organisation with confidence that it is compliant with its obligations, including that personal information is properly disposed of once mandated retention periods have elapsed. This also extends to third party service providers, meaning it is critical that organisations work with partners who are aware of their own obligations under the Privacy Act when it comes to how their clients' personal information is managed and disposed of.

Good governance ensures that not only is existing personal information managed appropriately, but that all ongoing and future data collection and retention policies adhere to the revised Act.

Better principles for better outcomes

While much of the activity we expect to see in relation to the changing Privacy Act will be focused on compliance, there are significant benefits that can also come from taking a proactive stance to ensuring readiness for the coming changes.

By undertaking the steps of Discover, Unify and Govern, an organisation will improve the security of data and reduce risk of a breach by better understanding what personal information it has while providing assurance that it is compliant with requirements. This means that not only will it be less likely to draw the ire of the OAIC, but that its customers will be able to feel more secure in their dealings.

Beyond this benefit however is the possibility of achieving operational benefits, both in terms of reducing information management costs, and also in unlocking new service and revenue opportunities through better utilisation of information assets.

The Iron Mountain information transformation model includes three additional stages of maturity - Automate, Unlock and Maintain.

- Automate to harness the full power of AI to classify and connect your data, automate manual processes, enable audit-ready compliance, and make information accessible and useful.
- Unlock previously unseen value in your data – make more informed business decisions, uncover new revenue streams, and improve analytics.
- Maintain by implementing practices to ensure that your data and information is kept current, accurate and compliant, so that it can continue delivering value back to the organisation.

However, none of these stages can be successfully reached without first undertaking Discover, Unify, and Govern.

The importance of experience

Iron Mountain brings unparalleled expertise in both records management and data governance, with more than 70 years' experience assisting private and public sector organisations manage everything from paper archives to massive digital libraries.

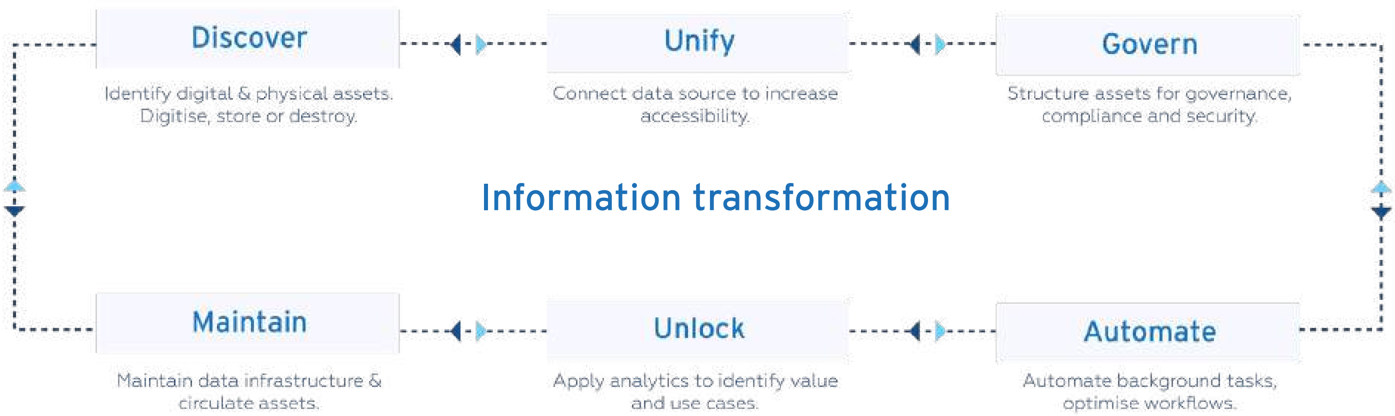
Importantly, our strong understanding of information lifecycle management ensures we can assist organisations achieve assurance and compliance, while our experience working with organisations around the world means we can bring innovative new thinking that can save costs and unlock new service opportunities.

With so much attention now given to the importance of properly maintaining privacy, the proposed changes to the Privacy Act may be only the beginning of a broader evolution in how personal information, and for that matter, all business information is maintained, which makes Iron Mountain the ideal partner for delivering your information maturity needs.

Start your information transformation with Iron Mountain

Let us help you prepare for the Privacy Act changes through a process we call, information transformation.

We help you discover, unify and govern your physical and digital assets so you can automate workflows, unlock valuable insights and maintain a compliant and digital-first approach to your organisation.



Iron Mountain solutions that will help get you there:

- Iron Mountain Smart Records Cleanup Suite - simplify, sort, and structure your records inventory automatically and at scale, and make smart decisions about what to keep, defensibly destroy, or digitise.
- Iron Mountain InSight® Digital Experience Platform - automate manual processes, enable audit-ready compliance, and make information accessible and useful with content management, intelligent document processing, workflow automation, and information governance capabilities.
- Iron Mountain Information Governance Advisory - combining technology with deep expertise and broad experience our information governance professionals can help you navigate the intricacies of retention, privacy, compliance and risk management.
- Iron Mountain Policy Centre - is a SaaS solution that provides you with expert guidance on changing regulations and privacy needs in accordance with your company's own customised data retention schedule.

IRON MOUNTAIN®

1300 476 668 | ironmountain.com/en-au

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

© 2024 Iron Mountain, Incorporated and/or its affiliates "Iron Mountain". All rights reserved. Information herein is proprietary and confidential to Iron Mountain and/or its licensors, does not represent or imply an invitation or offer, and may not be used for competitive analysis or building a competitive product or otherwise reproduced without Iron Mountain's written permission. Iron Mountain does not provide a commitment to any regional or future availability and does not represent an affiliation with or endorsement by any other party. Iron Mountain shall not be liable for any direct, indirect, consequential, punitive, special, or incidental damages arising out of the use or inability to use the information, which is subject to change, provided AS-IS with no representations or warranties with respect to the accuracy or completeness of the information provided or fitness for a particular purpose. "Iron Mountain" is a registered trademark of Iron Mountain in the United States and other countries, and Iron Mountain, the Iron Mountain logo, and combinations thereof, and other marks marked by ® or TM are trademarks of Iron Mountain. All other trademarks may be trademarks of their respective owners.