IRON MOUNTAIN®

White paper

Privacy Act Changes: Essential Governance Practices

Key Takeaways

- **Good data governance** is essential for compliance with Australia's changing privacy laws. Organisations need to know what data they have, where it is located, and how it is being used in order to comply with the new requirements.
- **A strong data governance framework** can help organisations to protect their data, improve its utility, and reduce risks. By establishing a clear set of policies and procedures for data management, organisations can ensure that their data is used in a responsible and ethical manner.
- **Organisations need to take a holistic approach to data governance.** They need to consider all of their data assets, both digital and physical, and they need to involve all stakeholders in the governance process
- **Data governance is not a one-time project, but rather an ongoing process.** Organisations need to continuously review and update their data governance policies and procedures to ensure that they remain relevant and effective.
- **Data is both an asset and a responsibility.** Organisations need to treat their data with care and respect, and they need to use it in a way that benefits both the organisation and its stakeholders.

Preparing for Privacy Act changes

Newly enacted and forthcoming changes to Australia's privacy regime are leading organisations of all sizes to question how they could be impacted and what the potential liability might be should they breach their obligations. These changes expand the definition of private information and set clearer guidance for how this data should be managed and how long it should be stored.

Ensuring compliance with these changing requirements demands that data is governed effectively.

But as many organisations are quickly learning, there is a significant gap between the storage and management of data and its effective governance.

The foundations of data governance

Data governance refers to the ability of an organisation to maintain both high-quality data and processes for managing that data throughout its entire lifecycle. This includes its classification, usage management, access privileges, security, and eventual destruction. The term "governance" specifically refers to the controls placed on data, encompassing guiding principles and actionable processes for management.

Good data governance not only ensures the organisation has access to high-quality data to pursue its goals, but also provides a solid understanding of what data it manages, as well as the value and liabilities associated with that data. This provides certainty that the organisation is in compliance with its privacy obligations and won't face surprises should it suffer a data breach or undergo regulatory scrutiny.

Benefits of a strong governance framework

Developing a strong data governance framework delivers multiple benefits:

1. **Enhanced data protection**: By understanding what data the organisation holds, it becomes possible to act with confidence, knowing that information is appropriately protected. Different levels of private information demand varying levels of security, particularly for sensitive topics such as health or financial records. Many organisations currently apply default levels of protection, which may lead to over- or under- defending certain data types.
2. **Improved data utility:** Identifying and classifying information makes it more useful. Organisations can't derive value from data they don't know exists or is inaccessible. Strong governance ensures high-value data is effectively managed and accessible.
3. **Risk reduction through disposal:** Once an organisation understands what privacy-related data it holds, it can reduce risks by disposing of data that's no longer required. Recent data breaches have shifted thinking toward minimising data retention. Disposing of redundant, obsolete, or trivial (ROT) data reduces liability and ensures compliance with statutory retention periods.
4. **Eliminating 'unknown unknowns':** By discovering and assessing all information for its privacy implications, leadership can ensure their repositories don't contain surprises that could surface during a cyber breach or regulatory investigation. This understanding also reduces financial liabilities by enabling more accurate risk assessment.

By establishing a strong data governance structure, it becomes possible to truly understand what the risks are, how to provision for them, and implement actions to potentially reduce those risks.

Creating a governance framework

Strong governance is enacted via a framework, which provides understanding regarding the organisation's regulatory environment and business requirements and the applicable obligations and the controls needed to meet them.

The first stage in creating a governance framework is to fully understand the privacy obligations that apply to the organisation, and that means fully comprehending the regulatory environment in which the organisation operates. This also means having a complete knowledge of the differentiating factors that set the organisation apart from others and how it retains and manages knowledge.

Many organisations will already have performed components of this assessment when complying with the Australian Corporations' Act, which requires them to define their industry and the regulations and directives that apply to them.

Once these factors are assessed and documented, it becomes possible to view privacy as a subset of its broader information resources. This act of demystification is one of the most important steps in creating a governance framework. It removes uncertainty around data retention and storage practices, enabling the organisation to build a framework that aligns with its needs as a regulated entity.

This assessment also provides the basis for breaking down the types of privacy-related data within the organisation. Through this process, the organisation will begin uncovering all the privacy-related information that it stores. This breaks down into two categories:

- Information or records that relate specifically to an individual, such as payroll and human resources records, or loyalty membership records for customers. In the case of health industry organisations, these might include patient records.
- Other information or records that include elements of private information, such as a shipping note that contains an individual's home address, or a sales database that contains the names of purchasers.

Putting governance in place

Establishing effective data governance requires a structured process to ensure assets are identified, connected, and managed in line with regulatory and business requirements. This process can be broken down into three critical steps: **Discover, Unify, and Govern.**

1 Discover

The first step is to identify both digital and physical assets. This involves determining what data exists, assessing its relevance, and deciding whether to digitise, securely store, or destroy it. By doing so, organisations gain a clear understanding of their information landscape while reducing unnecessary data liabilities.

2 Unify

Next, organisations must connect disparate data sources to improve accessibility and usability. Integrating data ensures that the right information is available to the right people at the right time. This step not only improves operational efficiency but also establishes a foundation for better compliance and decision-making.

3 Govern

Finally, organisations must implement structures to ensure compliance, security, and lifecycle management. This includes classifying data, defining retention and disposal policies, and establishing robust access controls. A well-structured governance framework provides a continuous improvement loop that adapts to evolving regulations and organisational needs.

Governance doesn't just apply in a single market, however. Developed countries around the world have their own data handling and privacy protection requirements, and while these are often standards-based, there are nuances that can trip up multinational organisations, especially when it comes to moving personal data between markets. As a global organisation, Iron Mountain has a strong understanding of each of these jurisdictions and the individual regulatory requirements that define best practices in data governance, ensuring that customers can remain compliant in whatever markets they operate.

Overcoming the data governance challenge

For many organisations, data governance challenges arise due to rapid digitisation and a lack of responsibility for maintaining data quality and controls. Data is often treated as a purely technical challenge, with emphasis on availability and storage rather than its value and associated risks.

Strong governance ensures data is both an asset and a responsibility, allowing leaders within the IT function to minimise risks while maximising the utility of their information. IT leaders play a critical role in making governance the cornerstone of their organisation's data strategy, transforming IT into a key enabler of business goals.

Leveraging information transformation for governance excellence

At Iron Mountain, we support organisations through all three critical steps: **Discover, Unify, Govern.** With our unique tools and expertise, we help organisations identify gaps in their governance programs and assess existing practices against best practices so they can implement effective controls for data discovery, retention, and compliance.

Our team of governance experts support organisations to address gaps and align with regulatory standards, enabling a continuous improvement process that ensures long-term compliance and governance success.

The governance windfall

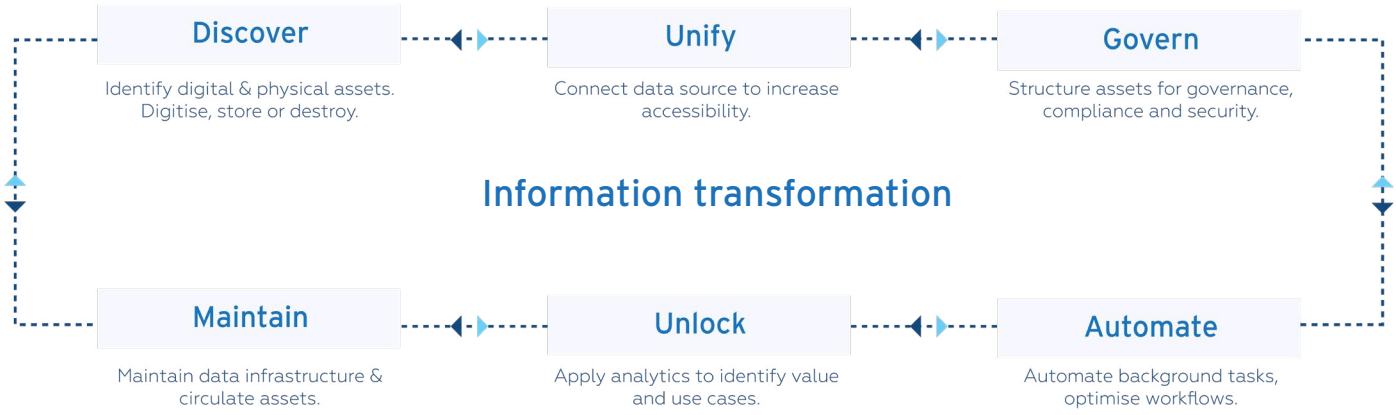
As data volumes grow and privacy requirements tighten, maintaining good data governance has become a critical necessity. When implemented correctly, governance delivers significant benefits, including reduced risks, lower data storage costs, and increased accessibility to high-value information.

By understanding their data assets, organisations can act with certainty and eliminate unknowns, ensuring they are managing and protecting data appropriately. Ultimately, this enables business leaders to make informed decisions, reducing surprises and aligning their operations with regulatory requirements.

Start your information transformation with Iron Mountain

Let us help you remain compliant with the new changes to the Privacy Act 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®

Contact us today to learn more about how strong governance practices can transform your organisation.

Visit our website to find out more>>

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.