Australian Information
Industry Association

Australian Information Industry Association
Submission on
Commonwealth Data Retention Review

21 March 2025

Introduction

The Australian Information Industry Association (AIIA) welcomes the opportunity to contribute to the Commonwealth Data Retention Review being undertaken by the Department of Home Affairs and the Attorney-General's Department (the Departments).

As the peak body for Australia's technology sector, the AIIA supports the intention to ensure data retention obligations remain appropriate, proportionate, and fit for purpose in a rapidly evolving digital and regulatory environment.

Since the introduction of the data retention framework, there have been significant shifts in the technology landscape, including the widespread adoption of cloud services, the growing importance of personal data governance, and evolving cyber security risks. These developments have highlighted the need to modernise regulatory requirements to ensure they are clear, consistent, and aligned with current operational practices and citizen expectations.

This submission outlines key considerations and opportunities for reform, including support for more targeted retention settings, improved clarity around cloud environments, proportionate obligations for SMEs, and better alignment with initiatives such as Digital ID and the Consumer Data Right.

Context and Vision: Personal Data Sovereignty and Governance

The AIIA advocates for reforms that are grounded in the principle of personal data sovereignty and governance —where citizens retain meaningful control over their personal information via informed consent. In this context, we support the proposed principles in the Discussion Paper, particularly Principle 1 (Minimisation) and Principle 5 (Necessity).

We also see an opportunity to introduce a first-principle of focusing on citizen experience and personal data control. The AIIA supports a whole-of-government approach, where initiatives such as the Digital Identity program and Consumer Data Right (CDR) provide secure, user-driven mechanisms to verify identity and share data with trusted parties. This enables consumers to compare and switch services with ease while retaining ownership of their information.

Singapore provides a useful reference. Its integration of SingPass (a digital ID equivalent) and MyInfo (a CDR equivalent) [1] [2] [3] allows citizens to transact seamlessly with both government and business. For instance, when applying for a credit card, a user can scan a QR code, authenticate via SingPass, and selectively authorise which data to share. With

[1] National Digital Identity Engagement Office Singapore, TechUP Series Webinar(Singpass and MyInfo for Seamless Service Delivery)-Assurity Trusted Solutions (2023).
[2] Smart Nation Singapore, Factsheet – Singpass (Singapore's National Digital Identity) (2022).
[3] GovTech Singapore, Singpass Myinfo – eKYC and form-filling made easier (2023).

over 800 organisations and 2,700 services onboarded, SingPass has supported over 500 million transactions to date.

Key privacy features of MyInfo include:

- Data minimisation by default—only necessary information is requested for each service.
- Automatic deletion of data if an application is not submitted.
- Transparent access logs allowing users to track data usage and access history via the SingPass app.

The AIIA recommends that the Departments consider the Singapore model as a reference point for enhancing Australia's Digital ID system and expanding the CDR. Such a model supports data minimisation, enables revocation of consent and access, and provides users with meaningful oversight of their data.

Key Challenges

Opaque Data Retention Requirements

A key challenge is the lack of clear justification for certain retention mandates. In many cases, it is unclear why specific types of data must be retained for extended periods, particularly when national security, law enforcement, or consumer protection objectives are not explicitly stated. This lack of clarity forces businesses to take a conservative approach, retaining large volumes of data longer than necessary to mitigate the risk of non-compliance. This not only drives up storage and compliance costs but also increases exposure to cyber security threats, as excess data storage becomes a target for malicious actors.

This issue is exemplified in the Optus 2022 incident in which the operator of critical (telecommunications) infrastructure had opaque and complex obligations under the myriad of regulations, including the Telecommunications Act and numerous supporting co-regulatory codes that the Australian Communications and Media Authority (ACMA) oversees.[4] Paradoxically, due to the incident, Optus now has even more need to retain data due to additional reporting requirements under ACMA and the upcoming Cyber Incident Review Board set up by the new Cyber Security Act, unless the Government streamlines this requirement.

To address these concerns, the Review should prioritise improved coordination between government agencies and clearer data retention requirements in procurement processes, as provided for in proposed Principle 4. Enhancing collaboration between regulators will ensure consistent enforcement and minimise duplication of reporting and compliance

[4] Tom Burton, Optus rings the data reform bells, Australian Financial Review (30 September 2022)

requirements. Retention mandates should also be clearly justified and aligned with specific policy objectives, providing clarity on why data must be retained and for how long. Addressing these issues will reduce unnecessary compliance burdens while ensuring data retention policies remain effective and proportionate.

Non-personal Data and Security Logging in Cloud Services

Security logging is a critical component of cyber security, enabling organisations to detect, investigate, and respond to cyber threats effectively. However, data retention requirements for security logs often create operational and compliance challenges, particularly in cloud environments where storage and processing costs are significant considerations. A common expectation in regulatory and procurement settings is a 24-month retention period for system and security logs. While extended retention can support forensic investigations and regulatory audits, it may also impose undue financial and technical burdens on industry, particularly cloud service providers that manage high volumes of log data across distributed systems. In practice, cloud providers typically adopt a risk-based approach to log retention, aligning with guidance from the Australian Cyber Security Centre (ACSC).

The AIIA supports the ACSC's Information Security Manual (ISM) control 1988, which recommends a minimum retention period of 12 months for security event logs, providing a balanced approach that supports both cyber resilience and operational efficiency. This guidance recognises that the security value of logs diminishes over time while the costs and risks associated with prolonged storage—such as increased attack surfaces and regulatory complexities—continue to grow.

Clarifying Archives Act Compliance for Cloud Services

Compliance with the Archives Act[5] presents a unique challenge in cloud environments, particularly in the absence of clear guidance on what constitutes an official record. Many procurement requests include generic requirements for cloud service providers to comply with the Act, but these requirements often lack specificity, leading to uncertainty and inefficiencies in compliance. Without clear parameters, businesses are left to interpret their compliance obligations independently, leading to inefficiencies, excessive data retention, and increased cyber security risks.

The complexity of Archives Act compliance in cloud environments stems from the diverse nature of digital records. Cloud-based services generate, store, and process a vast array of data types, including emails, documents, meeting recordings, chat logs, and system events. However, not all data generated within a cloud service should be classified as an official record requiring retention. The absence of clear definitions or sector-specific guidance leads many organisations to adopt an overly cautious "retain everything" approach, significantly increasing storage costs and exposure to data breaches.

[5] *Archives Act 1983* (Cth).

Additionally, the dynamic nature of cloud services—where data is frequently accessed, modified, and transferred across systems—compounds the challenge of meeting rigid retention requirements. Legacy regulations that were designed for traditional on-premises record-keeping do not always align with modern cloud-based architectures, creating compliance burdens that may not effectively contribute to the intended objectives of data retention.

The AIIA supports proposed Principle 5 in the Discussion Paper, which emphasises that retention provisions should specify only the information necessary to be retained and that data retention obligations should be clearly defined to provide certainty and prevent unnecessary data accumulation. It is crucial to establish explicit criteria for what constitutes an official record in a cloud environment, distinguishing between operational data, transient system logs, and records requiring long-term preservation. By modernising guidance and aligning it with the realities of cloud computing, the Review can help ensure that Archives Act compliance is both practical and effective, reducing regulatory uncertainty while maintaining appropriate records management practices.

Opportunities

Guidance and Proportionate Requirements for SMEs

Small and medium-sized enterprises (SMEs) face unique challenges in meeting data retention obligations due to limited resources, technical expertise, and financial constraints. Unlike larger corporations with dedicated compliance teams, SMEs often lack the capacity to implement complex data governance frameworks, leading to either over-retention of data due to uncertainty or non-compliance due to unawareness of specific requirements. The AIIA supports a proportionate approach to data retention for SMEs, ensuring that compliance obligations are both practical and scalable. Unclear or overly burdensome retention policies may divert SMEs' resources away from core business operations while increasing their exposure to cyber security risks if unnecessary data is stored without adequate protections. To support SMEs in managing their data retention obligations effectively, the AIIA recommends:

- **Clear, Practical Guidance for SMEs**: Government agencies should develop simplified, industry-specific guidelines to help SMEs understand their data retention responsibilities and implement best practices proportionate to their operational risks.
- **Encouragement of Cost-Effective Cyber Security Measures**: SMEs should be provided with access to resources, templates, and tools that facilitate secure data retention and disposal, reducing the likelihood of unnecessary data accumulation and cyber security vulnerabilities.

- **SME-Specific Training and Awareness Campaigns**: Government-led initiatives should focus on educating SMEs about their data retention obligations, providing practical steps for secure storage, retention, and disposal of information.

By ensuring that data retention policies account for the operational realities of SMEs, the Review can support compliance while preventing unnecessary regulatory burdens. A targeted, risk-based approach will enable SMEs to maintain compliance in a cost-effective and secure manner, reducing both their administrative overhead and exposure to cyber security threats.

Government as a Leader in Data Governance

As a major data holder and regulator, government has a dual responsibility: to model best-practice data governance and to uphold the same (or higher) standards it expects of private industry. According to the scope of this review, the AIIA recommends the Departments to consider how it could develop a best practice personal data governance model like the abovementioned SingPass/myInfo.

Conclusion

The AIIA appreciates the government's commitment to reviewing data retention obligations to ensure they remain effective, proportionate, and aligned with modern technology and risk environments. We recommend a first-principle approach in ensuring the reforms empower personal data sovereignty and governance.

We support a regulatory approach that is clear in its objectives, provides certainty for individuals and industry, and reflects the practical realities of data storage and use across both government and private sectors. This includes ensuring that compliance settings are scalable for smaller businesses, consistent across agencies, and informed by evolving technology and security needs.

We welcome the opportunity to continue working collaboratively with the Department of Home Affairs, the Attorney-General's Department, and other stakeholders to support the development of a contemporary and balanced data retention framework.

Should you require further information, please contact Ms Siew Lee Seow, General Manager, Policy and Media, at siewlee@aiia.com.au or 0435 620 406, or Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Thank you for considering our submission.

Yours sincerely
Simon Bush
CEO, AIIA

***

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies