Executive Summary

The Australian Retailers Association (ARA) welcomes the opportunity to provide a submission in response to the Commonwealth Government's Data Retention Review. As a $430 billion sector employing over 1.4 million Australians, the retail industry manages large volumes of customer, employee, and transaction data, making clear and consistent data retention requirements essential for operational efficiency and compliance.

Retailers face significant challenges in meeting current data retention obligations due to overlapping and inconsistent legislative requirements at the Commonwealth, state, and territory levels. The Privacy Act's vague "as long as necessary" standard conflicts with more prescriptive requirements under other statutes such as the Corporations Act, the Australian Consumer Law (ACL), and sector-specific regulations. This creates uncertainty for retailers, who often retain data for longer periods than necessary to avoid compliance risks — increasing operational costs and exposure to data breaches.

The ARA supports the draft Data Retention Principles as a foundation for reform. Aligning data retention requirements with the broader objectives of the Privacy Act Review and the Australian Cyber Security Strategy would create a more consistent, secure, and business-friendly framework. The Privacy Act Review aims to improve clarity and consistency in handling personal information, while the Cyber Security Strategy focuses on strengthening data protection and reducing breach risks. A modernised data retention framework would directly support both these objectives by providing clearer guidelines for retailers on how long data should be retained, how it should be destroyed, and how to reconcile conflicts between different statutory obligations.

Key areas of focus for the retail sector include:

- **Specifying retention periods** — Providing clear, defined retention periods for key data types would reduce ambiguity and allow retailers to implement consistent internal policies. This would support the Privacy Act Review's goal of improving compliance certainty and the Cyber Security Strategy's goal of reducing data exposure.
- **Alignment across jurisdictions** — Harmonising retention requirements between Commonwealth and state-based laws would reduce compliance complexity for national retailers and improve operational efficiency.
- **Data minimisation and destruction** — Providing clear guidance on when and how data should be deleted would enable retailers to reduce retained data volumes and strengthen data security, consistent with the Cyber Security Strategy's focus on improving breach response and recovery.
- **Safe harbour provisions** — Protecting retailers from liability when they delete data in line with approved guidance would increase confidence in implementing data minimisation strategies and improve compliance certainty.
- **Sector-specific guidance** — Retailers manage diverse types of data — including customer identity data, employee records, and sales records. Tailored guidance on how retention principles apply to these data types would improve practical compliance.

The ARA recommends that the government provide sector-specific guidance for retailers on how data retention principles apply to customer records, employee data, and transaction histories. Consistency with international frameworks, such as the European Union's General Data Protection Regulation (GDPR), would further simplify compliance for retailers operating in global markets and improve customer trust.

By addressing these issues, the government can establish a modern, risk-based data retention framework that balances consumer protection with the operational realities faced by Australian retailers. This would reduce compliance costs, improve data security, and strengthen Australia's broader data protection framework in line with both the Privacy Act Review and the Australian Cyber Security Strategy.

Response to Draft Principles

1. Principle 1 – Necessity and Minimisation

The ARA supports this principle as it would help retailers reduce the volume of stored personal data, lowering the risk of data breaches and minimising compliance costs. Currently, the Privacy Act's broad "as long as necessary" standard creates uncertainty for retailers about how long data should be retained. Retailers often default to retaining data for longer periods to avoid non-compliance, which increases breach exposure and storage costs. Providing clear guidance on when data can be deleted following verification or once legal requirements have been met would reduce ambiguity and allow retailers to confidently minimise retained data volumes.

Further, excessive retention periods for data such as employee records increase operational costs and compliance complexity for retailers. For example, the Administrative Functions Disposal Authority (AFDA) Express Version 2, issued by the National Archives of Australia, requires that employment records for employees who commenced work before the age of 18 be retained for 100 years from the employee's date of birth. Aligning these retention periods with practical business needs would reduce storage costs and administrative burdens while maintaining appropriate protections for sensitive employment data.

Distinguishing between high-risk and low-risk data would further improve compliance certainty. High-risk data, such as financial transaction records and identity verification data, may need to be retained longer to meet legal and regulatory requirements. In contrast, low-risk data, such as customer marketing preferences and product browsing history, could be retained for shorter periods without creating legal risk. Allowing shorter retention for low-risk data would reduce data storage costs and limit the fallout from potential data breaches.

Considerations:

The Privacy Act's ambiguity around "necessary" retention periods conflicts with other legislative requirements, such as the Corporations Act and Australian Consumer Law (ACL). Greater alignment between the Privacy Act and other statutory requirements would enable retailers to implement automated deletion systems without the risk of inadvertently breaching compliance obligations.

The government should clarify that real-time identity verification through the Document Verification Service (DVS) satisfies record-keeping requirements under relevant laws. Currently, In South Australia, the General Code of Practice Guidelines issued by Consumer and Business Services (CBS) require that records of alcohol deliveries — including the type of identification, recipient's name, date of birth, and delivery address — must be retained for at least one year following delivery. Removing this redundancy would reduce retained data volumes and breach exposure.

Further, proposed reforms to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) could extend coverage to high-value retailers, such as jewellers. If implemented, these reforms would require businesses to retain customer identity records for seven years after the customer relationship ends — even if the customer's identity was verified using DVS. This would create a conflict with the Privacy Act's data minimisation principle, as businesses would be forced to store sensitive identity information long after the transaction is complete. Clarifying that DVS verification satisfies AML/CTF record-keeping requirements would prevent this conflict and reduce data retention volumes.

2. Principle 2 – Specified Periods

The ARA supports this principle as it would provide retailers with greater certainty about how long different types of data should be retained. Currently, retailers face inconsistent retention periods under different statutes, which creates compliance uncertainty and increases operational costs. This forces many retailers to default to the longer period to avoid non-compliance, which increases storage costs and breach exposure. Clear and consistent retention periods would allow retailers to adopt uniform data management practices, improve operational efficiency, and reduce the volume of data at risk in the event of a breach.

Specifying consistent retention periods would further support the adoption of automated deletion systems, which are difficult to implement under the current framework due to conflicting retention requirements. Greater certainty would allow retailers to automate data destruction once the retention period expires, reducing manual oversight and improving compliance.

Considerations:

While defined retention periods would provide greater certainty, retailers should also have the flexibility to retain data for legitimate commercial purposes beyond the minimum period where appropriate privacy safeguards are applied. For example, retailers may need to retain customer transaction data for longer periods to manage loyalty programs or to provide customer support beyond the statutory requirement. Retention policies should allow retailers to meet both regulatory and commercial needs without creating compliance conflicts.

Sector-specific guidance would further improve the practical implementation of this principle. The retail sector handles diverse data sets — including customer identity information, transaction data, and employee records — which may require different retention approaches. For example, customer loyalty data may not need to be retained as long as financial transaction records linked to tax obligations. Providing tailored guidance for the retail sector would enable businesses to implement consistent policies while accommodating industry-specific requirements.

Finally, retailers would benefit from guidance on how to handle historical data retained under outdated requirements. Allowing businesses to apply updated retention periods retroactively would reduce the need to store legacy data that no longer serves a business or regulatory purpose.

3. Principle 3 – Alignment

The ARA supports this principle as it would simplify compliance for retailers operating across multiple jurisdictions. Currently, retention periods for similar types of data — such as CCTV footage, employee records, customer identity data and contracts under seal— vary between Commonwealth, state, and territory laws. This forces retailers to maintain different internal retention policies depending on the jurisdiction, increasing administrative complexity and compliance risk. National consistency would allow retailers to adopt uniform retention policies across their operations, improving efficiency and reducing compliance costs.

Alignment would also support the adoption of automated data retention and deletion systems. Currently, inconsistencies between Commonwealth and state laws prevent retailers from automating deletion processes, as the same type of data may need to be retained for different periods in different jurisdictions. Establishing a single national standard would remove this barrier and allow for greater adoption of automated systems.

Greater alignment would also support the broader objectives of the Privacy Act Review and the Australian Cyber Security Strategy. The Privacy Act Review emphasises the need for consistency and clarity in handling personal information, while the Cyber Security Strategy highlights the importance of reducing retained data volumes to improve breach response and

data protection. Establishing a nationally consistent retention framework would reduce data over-retention and improve retailers' ability to secure retained data — directly supporting both policy priorities.

Retailers also face challenges in balancing differing commercial client expectations with legislative and contractual requirements. For example, retailers that provide additional financial services or operate loyalty programs often need to comply with conflicting data retention requirements from different regulatory bodies and commercial partners. Greater alignment between Commonwealth, state, and contractual requirements would improve operational efficiency and reduce legal uncertainty.

Considerations:

Greater alignment between Commonwealth and state laws is essential for improving operational certainty. For example, some state-based liquor licensing laws still require proof of identity verification to be retained even if the DVS has already verified a customer's identity. This creates operational complexity and increases retained data volumes unnecessarily.

The government should clarify how to reconcile conflicts between the Privacy Act's minimisation principle and longer retention periods required under other statutes such as the Corporations Act and the Australian Consumer Law (ACL). Providing a clear order of precedence would allow retailers to apply consistent data retention policies without the risk of non-compliance.

Aligning data retention requirements with international frameworks such as the European Union's General Data Protection Regulation (GDPR) would further simplify compliance for retailers operating in global markets. The GDPR's consistent approach to retention periods and data minimisation has provided businesses with greater certainty and reduced compliance costs. A similar approach in Australia would support operational efficiency and improve customer trust.

4. Principle 4 – Data Destruction

Overall Position:

The ARA supports this principle as it would reduce data volumes, lower breach risks, and improve compliance certainty for retailers. Currently, there is no consistent framework for secure data destruction. Retailers often retain data longer than necessary due to uncertainty about whether they are legally permitted to delete it. The Privacy Act's "as long as necessary" standard increases this ambiguity, leading to over-retention and increased breach exposure. Clear guidelines on acceptable data destruction methods — including encryption, physical destruction, and secure deletion — would give retailers confidence to reduce stored data volumes.

Considerations:

The government should clarify how destruction requirements apply to different data types. For example, customer identity data may require stricter destruction methods (e.g., encryption-based deletion) than employee shift records or marketing preferences. Providing differentiated guidance would help retailers develop secure and efficient destruction policies.

Aligning destruction guidance with existing cybersecurity standards (e.g., the Australian Cyber Security Centre's guidelines) would improve consistency and reduce breach risks. The government should also address the handling of backup and archived data, as legacy systems may retain copies of deleted data unless explicitly covered by destruction guidance.

A safe harbour provision should again apply where destruction is carried out in line with government guidance. If a retailer securely deletes customer data using an approved method after the specified retention period, they should not face penalties if a legal challenge arises. This would give retailers the confidence to destroy data promptly without fearing regulatory consequences.

5. Principle 5 – Clear Definition of Data Types

Overall Position:

The ARA supports this principle as it would give retailers greater certainty when handling different types of data. Currently, there is no clear definition of customer, employee, financial, and transactional data under the Privacy Act, leading to inconsistent retention practices and increased breach exposure. Defining different data categories would allow retailers to implement differentiated retention periods based on the type and sensitivity of the data.

For example, customer identity data used for age verification may need to be retained for longer periods under liquor licensing laws, whereas marketing preferences or product browsing history could be deleted after a shorter period. Defining these categories would enable retailers to apply consistent policies and improve compliance certainty.

Considerations:

The government should provide specific definitions for key data categories, including financial records, employee data, customer identity data, and marketing information. For example, purchase history data may require different retention treatment from warranty or loyalty program data. Clear definitions would reduce ambiguity and support consistent retention and deletion practices.

Where definitions conflict with other legislative requirements (e.g., the Corporations Act or AML/CTF Act), the government should clarify the order of precedence. This would allow retailers to develop a single, consistent retention policy without needing to adjust for conflicting requirements.

Conclusion

The ARA supports the government's objective to establish a clearer, more consistent data retention framework. The draft principles provide a strong foundation for reform, but further detail and targeted guidance are needed to address the practical challenges faced by retailers.

Inconsistent retention periods remain a key challenge. Greater consistency between Commonwealth and state requirements would simplify compliance and reduce operational costs for retailers. Aligning retention requirements with the objectives of the Privacy Act Review and the Australian Cyber Security Strategy would further strengthen data security and improve compliance certainty.

Clear guidance on data destruction is essential. Retailers retain data longer than necessary due to uncertainty about acceptable deletion methods and the handling of backups. Establishing consistent standards for secure data destruction would reduce breach exposure and improve compliance confidence.

Introducing a safe harbour provision would further support data minimisation strategies. Retailers that delete data in line with approved guidance should be protected from liability if a dispute arises, giving businesses greater confidence to reduce retained data volumes.

Providing sector-specific guidance on managing customer identity data, employee records, and sales data would improve compliance certainty and reduce ambiguity. Aligning Australia's data retention framework with international standards, such as the GDPR, would simplify compliance for multinational retailers and improve customer trust.