SLICIFY

Data Retention Policy

Effective Date: April 2026

Version 1.0

1. Purpose and Scope

This Data Retention Policy sets out Slicify's obligations and practices regarding the retention and deletion of personal information and business data. It applies to all employees, contractors, and third parties who handle data on behalf of Slicify.

Slicify is committed to retaining data only for as long as necessary and disposing of it securely when it is no longer needed. This policy supports our compliance with:

- The New Zealand Privacy Act 2020 (Information Privacy Principle 9)
- The Australian Privacy Act 1988 (Australian Privacy Principle 11.2)
- Applicable tax, employment, and corporate record-keeping legislation in New Zealand and Australia

2. Principles of Data Retention

Slicify adheres to the following principles when determining how long to retain data:

- Necessity: Data is retained only for as long as it is needed for the purpose for which it was collected, or as required by law.
- Proportionality: Retention periods are proportionate to the sensitivity of the data and the risk of harm from inappropriate retention.
- Accountability: Clear ownership is assigned for data retention decisions and disposal actions.
- Security: Data is stored securely throughout its retention period and disposed of securely at the end.
- Transparency: Individuals are informed of how long their data will be retained in our Privacy Policy.

3. Retention Schedule

The following table sets out the standard retention periods for the main categories of data held by Slicify. These periods represent the minimum retention period. Specific circumstances (e.g., litigation hold) may require longer retention.

Data Category	Retention Period	Legal Basis / Notes
Customer account data	Duration of relationship + 7 years	Contractual obligation and tax law
Financial and billing records	7 years	NZ Companies Act / Australian

Data Category	Retention Period	Legal Basis / Notes
		tax law
Contracts and agreements	7 years after expiry	Limitation of actions legislation
Employee personal data	7 years after employment ends	Employment law and tax obligations
Job applicant data (unsuccessful)	12 months	Discrimination law compliance
Marketing contact data	Until consent withdrawn + 1 year	Privacy Act consent requirements
Website analytics and logs	13 months	Security monitoring purposes
Support tickets and communications	3 years	Service quality and dispute resolution
AI model training data (identified)	Duration of consent + 2 years	Explicit consent required
AI model training data (de-identified)	Indefinite	No longer personal information
Security incident logs	5 years	Security and legal obligations
Backup data	As per primary retention + 30 days	Disaster recovery purposes

4. Litigation Hold

Where Slicify is involved in, or anticipates involvement in, any legal dispute, regulatory investigation, or audit, the normal retention schedule is suspended for relevant data. A litigation hold notice will be issued by the Legal/Compliance team, specifying which data must be preserved and for how long.

Employees must not destroy any data subject to a litigation hold until the hold is formally lifted.

5. Data Disposal

5.1 Secure Disposal Methods

When data has reached the end of its retention period (and is not subject to a litigation hold), it must be disposed of securely:

- Electronic data: Secure deletion using approved data wiping tools that overwrite data to industry standards (e.g., NIST 800-88 guidelines)
- Cloud data: Deletion via secure API calls or management consoles, followed by verification of deletion from backups within the retention period
- Physical documents: Cross-cut shredding by approved destruction services with a certificate of destruction
- Storage media (hard drives, USB drives): Physical destruction or degaussing by certified providers

5.2 Disposal Records

Records of all data disposal activities must be maintained, including the date of disposal, the category and volume of data disposed of, and the method used. These records are retained for 3 years.

6. Roles and Responsibilities

- Privacy Officer: Oversees compliance with this policy, approves retention schedules, and manages exception requests.
- Department Managers: Responsible for ensuring their teams comply with retention schedules and report any issues to the Privacy Officer.
- IT/Systems Team: Implements technical controls for automated data deletion and maintains secure disposal processes.
- All Employees: Responsible for handling data in accordance with this policy and reporting any breaches or concerns.

7. Review and Exceptions

This policy is reviewed annually or when significant changes occur in law, technology, or business operations. Requests for exceptions to the standard retention schedule must be submitted to the Privacy Officer in writing, with clear justification.

All exceptions are documented and approved in writing before any deviation from this policy is permitted.

8. Breaches

Any failure to comply with this policy may constitute a breach of the NZ Privacy Act 2020 or the Australian Privacy Act 1988 and may result in disciplinary action. Data retained beyond its permitted period, or data not disposed of securely, must be reported to the Privacy Officer immediately.

9. Related Policies

- Privacy Policy
- Information Security Policy
- Incident Response Plan

10. Contact

For questions about this policy, contact:

- Privacy Officer, Slicify
- Email: privacy@slicify.ai