



Data Retention and Deletion Policy

Gibble SaaS Platform

Prepared by: Gregory Ibbotson – G.I. IT Security

Version: 1.0



Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

Table of Contents

1.	Purpose	3
2.	Scope	3
3.	3. Definitions	4
4.	Data Retention Principles	4
5.	Retention Periods	4
6.	Data Deletion Processes	5
7.	Data Subject Deletion Requests	6
8.	Security Measures	7
9.	Roles and Responsibilities	7
10.	Compliance and Auditing	8
11.	Incident Management	8
12.	Regional Considerations	9
13.	Contact Information	9

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

1. Purpose

1.1 This Data Retention and Deletion Policy ("Policy") outlines how Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), manages the retention, storage, and secure deletion of personal information and customer data processed through our SaaS platforms for learning, payroll, student management, and human resources management. The Policy ensures compliance with data minimisation and storage limitation principles under applicable data protection laws.

1.2 The Policy applies to all data processed on our platforms, hosted on Amazon Web Services (AWS) and Microsoft Entra infrastructure, and monitored by Adlumin Managed Detection and Response (MDR) services.

1.3 We are committed to complying with:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly APP 11.2.
- EU General Data Protection Regulation 2016/679 (GDPR), Article 5(1)(e).
- *Privacy Act 2020* (New Zealand), Information Privacy Principle (IPP) 9.
- Singapore Personal Data Protection Act (PDPA).
- California Consumer Privacy Act (CCPA/CPRA).
- Japan Act on the Protection of Personal Information (APPI).

1.4 For inquiries, contact our Data Protection Officer (DPO) at:

- Email: privacy@gibble.com.au
- Address: Level 2, Suite 204, 189E South Centre Rd, Tullamarine VIC 3043, Australia
- Phone: +61 3 9744 2887

1.5 This Policy is reviewed annually or as needed to reflect changes in regulations, business operations, or technology. Updates are posted at www.gibble.com.au/retention.

2. Scope

2.1 This Policy applies to:

- Personal information and customer data processed via Gibble's platforms, including names, contact details, payroll data, student records, biometric data, and analytics data.
- Data stored in AWS (e.g., S3, RDS), Microsoft Entra (e.g., Azure Blob Storage), on-premises systems, and third-party platforms (e.g., Salesforce, Stripe).
- Data held in physical formats (e.g., hard-copy files in Gibble's offices).

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

- Data subjects, customers, employees, and contractors in Australia, New Zealand, the EU, UK, Singapore, USA, and Japan.

2.2 It covers retention periods, deletion processes, and responses to data subject deletion requests, as referenced in the Privacy Policy (Sections 14, 17.5) and Security Policy (Section 5.5).

3. 3. Definitions

3.1 Personal Information: Any information relating to an identified or identifiable individual, including names, contact details, payroll data, biometric data, or IP addresses, as defined by applicable laws.

3.2 Customer Data: Data provided by or on behalf of customers, including end-user data entered into Gibble’s platforms or migrated from legacy systems.

3.3 Retention Period: The duration for which data is stored before deletion, based on legal, contractual, or operational requirements.

3.4 Secure Deletion: The process of permanently removing data to prevent recovery, using methods like cryptographic erasure or certified physical destruction.

4. Data Retention Principles

4.1 Data Minimisation: We retain personal information and customer data only for as long as necessary to fulfill the purposes outlined in our Privacy Policy or as required by law.

4.2 Purpose Limitation: Data is retained only for the specific purposes for which it was collected (e.g., platform functionality, billing, legal compliance).

4.3 Legal Compliance: Retention periods comply with applicable laws and customer contracts, balancing regulatory requirements with data subject rights.

4.4 Secure Storage: Data is stored securely using AES-256 encryption for data at rest and TLS 1.3 for data in transit, as per the Security Policy (Section 5.2).

5. Retention Periods

5.1 The following table outlines retention periods for key data categories, subject to legal and contractual requirements:

Data Category	Retention Period	Rationale
Customer Personnel Data (e.g., names, contact details, billing information)	7 years after contract termination	Australian tax law requires 7-year retention for financial records; GDPR

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

Data Category	Retention Period	Rationale
		allows retention for contractual obligations.
End-User Data (e.g., payroll, student records)	As specified in customer contracts or 7 years after account deletion, whichever is longer	Contractual obligations and legal requirements (e.g., Australian Taxation Office, GDPR Article 5).
Biometric Data (e.g., fingerprints for time tracking)	Until employee/contractor termination or explicit consent withdrawal, unless required by law	GDPR Article 9, APP 7 (sensitive data); deleted immediately upon consent withdrawal unless legally required.
Analytics Data (de-identified)	2 years	Aligns with Google Analytics retention settings and operational needs for platform improvement (Privacy Policy, Section 7).
Support and Security Data (e.g., IP addresses, access logs)	1 year	Necessary for security audits and incident response, per ISO 27001 and GDPR Article 32.
Employee/Contractor Data (e.g., HR records, tax file numbers)	7 years after employment/contract end	Australian tax and superannuation laws; GDPR allows retention for legal compliance.
Physical Records (e.g., hard-copy files)	7 years or as per customer contracts	Australian record-keeping laws; secure destruction thereafter.
Backup Data	90 days for incremental backups; 1 year for full backups	Ensures recovery capabilities (Security Policy, Section 5.5); complies with data minimisation.

5.2 Exceptions:

- Data required for legal proceedings (e.g., court orders) is retained until proceedings conclude.
- Data subject to regulatory audits (e.g., tax audits) is retained as required by law.
- Customer contracts may specify longer retention periods, which take precedence.

6. Data Deletion Processes

6.1 Electronic Data:

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

- Automated Deletion: AWS S3 lifecycle policies and Azure Blob Storage rules automatically delete data after retention periods expire.
- Manual Deletion: Data marked for deletion (e.g., upon account termination) is removed using cryptographic erasure (e.g., overwriting with random data).
- Database Deletion: Tenant-specific databases are purged using secure SQL commands, verified by the IT Manager.
- Backup Deletion: Expired backups are deleted via AWS Backup and Azure Backup policies, ensuring no residual data remains.

6.2 Physical Data:

- Hard-copy records are shredded using certified secure destruction services, with destruction certificates issued.
- Physical media (e.g., USB drives) are destroyed using industry-standard degaussing or physical shredding.

6.3 Third-Party Data:

- Third-party providers (e.g., Stripe, Salesforce) are instructed to delete data upon retention period expiry, per Data Protection Agreements (DPAs).
- Adlumin MDR logs are deleted after 1 year, unless required for ongoing investigations.

6.4 Verification:

- Deletion processes are audited quarterly to ensure no residual data remains.
- Adlumin MDR monitors for unauthorised data access post-deletion.

7. Data Subject Deletion Requests

7.1 Request Process:

- Data subjects can request deletion via:
 - Their customer (e.g., employer or platform administrator), as per Privacy Policy (Section 14.2).
 - Directly to Gibble at privacy@gibble.com.au or through www.gibble.com.au/rights.
- Requests must include sufficient information to verify identity (e.g., account details, ID documents).

7.2 Response Timeline:

- Australia: Within 30 days (APP 13).
- EU/UK: Within 1 month, extendable by 2 months for complex requests (GDPR Article 12).

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

- New Zealand: Within 20 working days (IPP 7).
- Singapore, USA, Japan: Within 30 days or as required by PDPA, CCPA/CPRA, or APPI.

7.3 Exceptions:

- Deletion may be refused if data is required for legal obligations (e.g., tax records), contractual commitments, or ongoing legal proceedings.
- Refusals are communicated with reasons and escalation options (e.g., to the OAIC).

7.4 Execution:

- Approved requests trigger deletion from active databases and backups.
- Customers are notified to confirm deletion of their data subjects' information.
- A record of the request and deletion is maintained for audit purposes.

8. Security Measures

8.1 Storage Security:

- Data is encrypted using AES-256 for data at rest and TLS 1.3 for data in transit, as per the Security Policy (Section 5.2).
- Access is restricted via AWS IAM and Microsoft Entra role-based access controls with multi-factor authentication (MFA).

8.2 Deletion Security:

- Deletion processes prevent data recovery, using cryptographic erasure for electronic data and certified destruction for physical records.
- Adlumin MDR monitors for unauthorised attempts to access deleted data.

8.3 Backup Security:

- Backups are stored in encrypted AWS S3 buckets and Azure Blob Storage, with access restricted to authorised IT personnel.
- Backup deletion is logged and verified via AWS CloudTrail and Microsoft Defender for Cloud.

9. Roles and Responsibilities

9.1 Data Protection Officer (DPO):

- Oversees policy implementation and compliance.

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

- Handles data subject deletion requests and regulatory inquiries.
- Maintains retention and deletion records.

9.2 Security Officer:

- Monitors deletion processes via Adlumin MDR and AWS/Microsoft tools.
- Ensures secure deletion of sensitive data (e.g., biometric data).

9.3 IT Manager:

- Configures AWS S3 and Azure Blob Storage lifecycle policies.
- Executes manual deletions and verifies completion.

9.4 Customers:

- Specify retention periods in contracts, where applicable.
- Notify Gibble of data subject deletion requests, as per Privacy Policy (Section 14).

9.5 Employees and Contractors:

- Comply with retention and deletion procedures.
- Report suspected data retention violations to security@gibble.com.au.

10. Compliance and Auditing

10.1 Compliance:

- The Policy aligns with ISO 27001 A.12.3 (backup) and A.18.1.3 (protection of records).
- AWS and Microsoft Entra compliance dashboards track adherence to GDPR, APPs, PDPA, CCPA, and APPI.
- Adlumin MDR provides audit-ready logs for retention and deletion activities.

10.2 Auditing:

- Quarterly audits verify compliance with retention schedules and deletion processes.
- Annual third-party audits for ISO 27001 and SOC 2 Type II include retention policy reviews.
- Audit reports are available to customers upon request at security@gibble.com.au.

11. Incident Management

11.1 Retention Violations:

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025

- Unauthorised retention (e.g., data kept beyond retention periods) is treated as a security incident, per the Data Breach Response Plan (Section 10).
- Adlumin MDR detects and reports retention anomalies.

11.2 Breach Integration:

- If a data breach occurs, retention periods may be extended for affected data to support investigations, with regulatory notification as required (Data Breach Response Plan, Section 8).

12. Regional Considerations

12.1 Australia: 7-year retention for financial and tax-related data; deletion requests handled per APP 13.

12.2 EU/UK: Data retained only as long as necessary (GDPR Article 5); deletion requests processed within 1 month (extendable).

12.3 New Zealand: Retention aligns with IPP 9; deletion requests within 20 working days.

12.4 Singapore: PDPA requires reasonable retention periods; deletion within 30 days of request.

12.5 USA (CCPA/CPRA): Deletion requests processed within 45 days, with exceptions for legal obligations.

12.6 Japan (APPI): Retention limited to purpose of use; deletion requests handled per Article 30.

13. Contact Information

13.1 For inquiries or deletion requests, contact:

- **Data Protection Officer:** privacy@gibble.com.au
- **Security Officer:** security@gibble.com.au
- **Phone:** +61 3 9744 2887

13.2 Complaints can be escalated to:

- **Australia:** Office of the Australian Information Commissioner, enquiries@oaic.gov.au, 1300 363 992.
- **New Zealand:** Office of the Privacy Commissioner, enquiries@privacy.org.nz.
- **EU:** Relevant supervisory authority (e.g., ICO in the UK).
- **Singapore:** Personal Data Protection Commission, info@pdpc.gov.sg.
- **USA:** Relevant state authority (e.g., California Attorney General).
- **Japan:** Personal Information Protection Commission, info@ppc.go.jp.

Leftorium Pty Ltd (Trading as Gibble) Data Retention and Deletion Policy

Last updated: July 2025