Data Subject Rights Policy

Gibble SaaS Platform

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

Version: 1.0

Leftorium Pty Ltd
Suite 204, 189E South Centre Road, Tullamarine VIC 3043
Email: info@gibble.com.au | Phone: (03) 9744 2887

ABN 65 7612 792
Trading as **Gibble** - *gibble.com.au*

Leftorium Pty Ltd (Trading as Gibble) Data Subject Rights Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Data Subject Rights Policy

Last updated: July 2025

1. Purpose

1.1 This Data Subject Rights Policy ("Policy") outlines the procedures for handling requests from data subjects regarding their personal information processed by Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our") through our SaaS platforms for learning, payroll, student management, and human resources management. The Policy ensures data subjects can exercise their rights under applicable data protection laws.

1.2 The Policy integrates with our Privacy Policy (Sections 14, 17.6), Data Retention and Deletion Policy (Section 7), and other policies, leveraging Amazon Web Services (AWS), Microsoft Entra, and Adlumin Managed Detection and Response (MDR) services to securely manage data subject requests.

1.3 We are committed to compliance with:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly APPs 12 and 13.
- EU General Data Protection Regulation 2016/679 (GDPR), Articles 15-22.
- *Privacy Act 2020* (New Zealand), Information Privacy Principles (IPPs) 6 and 7.
- Singapore Personal Data Protection Act (PDPA).
- California Consumer Privacy Act (CCPA/CPRA).
- Japan Act on the Protection of Personal Information (APPI), Articles 27-32.

1.4 For inquiries or to submit a data subject request, 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
- **Website**: www.gibble.com.au/rights

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

2. Scope

2.1 This Policy applies to:

- Personal information processed through Gibble's platforms, including names, contact details, payroll data, student records, biometric data, and analytics data, as described in the Privacy Policy (Section 4).
- Data subjects, including customers' end users (e.g., employees, students), employees, contractors, and website visitors in Australia, New Zealand, the EU, UK, Singapore, USA, and Japan.
- Data stored on AWS (e.g., S3, RDS), Microsoft Entra (e.g., Azure Blob Storage), and third-party systems (e.g., Salesforce, Stripe).

2.2 It covers data subject rights, including access, correction, deletion, restriction, portability, objection, and automated decision-making, as applicable under relevant laws.

3. Definitions

3.1 **Data Subject**: An identified or identifiable individual whose personal information is processed by Gibble.

3.2 **Personal Information**: Information relating to a data subject, such as names, contact details, biometric data, or IP addresses, as defined in the Privacy Policy (Section 4).

3.3 **Data Controller**: The entity determining the purposes and means of processing personal information (typically Gibble's customers for end-user data).

3.4 **Data Processor**: Gibble, when processing personal information on behalf of customers, as per the Privacy Policy (Section 3).

4. Data Subject Rights

4.1 Data subjects may exercise the following rights, subject to applicable laws and exceptions:

- **Right to Access**: Obtain confirmation of whether their personal information is processed and access a copy of it (GDPR Article 15, APP 12, IPP 6).
- **Right to Correction**: Request correction of inaccurate or incomplete personal information (GDPR Article 16, APP 13, IPP 7).
- **Right to Deletion**: Request deletion of personal information when no longer necessary or unlawfully processed (GDPR Article 17, APP 13, IPP 7, CCPA/CPRA).
- **Right to Restriction**: Request restriction of processing under specific conditions (e.g., disputed accuracy) (GDPR Article 18).
- **Right to Data Portability**: Receive personal information in a structured, machine-readable format and transmit it to another controller (GDPR Article 20).
- **Right to Object**: Object to processing for direct marketing or legitimate interests (GDPR Article 21, PDPA, APPI).
- **Right Against Automated Decision-Making**: Not be subject to decisions based solely on automated processing, including profiling, with significant effects (GDPR Article 22).

4.2 Gibble does not engage in automated decision-making or profiling with legal or significant effects, as per the Privacy Policy (Section 7).

5. Request Process

5.1 **Submitting a Request**:

- Data subjects can submit requests via:
    - Their customer (e.g., employer, institution), who forwards the request to Gibble, per the Privacy Policy (Section 14.2).
    - Directly to Gibble via privacy@gibble.com.au or the online portal at www.gibble.com.au/rights.
- Requests must include:
    - Full name and contact details.
    - Description of the request (e.g., access, deletion).
    - Sufficient information to verify identity (e.g., account ID, government-issued ID for sensitive requests).

5.2 **Identity Verification**:

- Gibble verifies the data subject's identity using secure methods (e.g., account credentials, ID checks).
- For customer-managed end users, verification may be handled by the customer, with Gibble confirming customer authorisation.
- Verification processes comply with the Access Control Policy (Section 5).

5.3 **Response Timelines**:

- **Australia**: Within 30 days (APP 12, 13).
- **EU/UK**: Within 1 month, extendable by 2 months for complex requests (GDPR Article 12).
- **New Zealand**: Within 20 working days (IPP 6, 7).
- **Singapore**: Within 30 days (PDPA).
- **USA (CCPA/CPRA)**: Within 45 days for deletion/verification, 10 days for acknowledgment.
- **Japan**: Within a reasonable period (APPI Article 30).

5.4 **Exceptions**:

- Requests may be refused if:
    - The data subject's identity cannot be verified.
    - The request is manifestly unfounded or excessive (GDPR Article 12).
    - Legal or contractual obligations require data retention (e.g., 7 years for tax records, per the Data Retention and Deletion Policy, Section 5).
- Refusals are communicated with reasons and escalation options (Section 9).

6. Processing Requests

6.1 **Access Requests**:

- Provide a copy of the data subject's personal information in a secure, electronic format (e.g., encrypted PDF).
- Include details on processing purposes, data categories, recipients, and retention periods, per GDPR Article 15.
- Data is retrieved from AWS RDS, Azure Blob Storage, or third-party systems (e.g., Salesforce), per the Access Control Policy (Section 6).

6.2 **Correction Requests**:

- Update inaccurate or incomplete data in active databases and backups.
- Notify customers and third-party vendors (e.g., Stripe) to update data, per the Vendor Management Policy (Section 5).
- Confirm corrections to the data subject within the response timeline.

6.3 **Deletion Requests**:

- Delete data from active systems and backups, per the Data Retention and Deletion Policy (Section 6).
- Use cryptographic erasure for electronic data and certified shredding for physical records.
- Notify vendors to delete data, with verification of compliance.

6.4 **Restriction Requests**:

- Restrict processing by flagging data in systems (e.g., AWS RDS) to prevent further use.
- Maintain restricted data securely until the restriction is lifted or deletion is required.

6.5 **Portability Requests**:

- Provide data in a structured, commonly used, machine-readable format (e.g., JSON, CSV).
- Ensure secure transmission (e.g., encrypted email or secure portal).

6.6 **Objection Requests**:

- Cease processing for marketing or legitimate interests, if applicable.
- Disable non-essential cookies or analytics tracking, per the Cookie Policy (Section 5).

7. Security Measures

7.1 **Data Protection**:

- Personal information is protected during request processing with AES-256 encryption for data at rest and TLS 1.3 for data in transit, per the Security Policy (Section 5.2).

- Access to data is restricted via AWS IAM and Entra ID with MFA, per the Access Control Policy (Section 5).

7.2 **Monitoring**:

- Adlumin MDR monitors request-related activities for unauthorised access, per the Information Security Incident Management Policy (Section 6).
- AWS CloudTrail and Microsoft Defender for Cloud log access events.

7.3 **Incident Handling**:

- Any security incidents during request processing are managed per the Information Security Incident Management Policy (Section 8) and Data Breach Response Plan (Section 7).

8. Roles and Responsibilities

8.1 **Data Protection Officer (DPO)**:

- Oversees request processing and compliance.
- Responds to data subject inquiries and escalates complex cases.
- Maintains records of requests for audits.

8.2 **Security Officer**:

- Ensures secure access to data during request processing.
- Monitors for incidents via Adlumin MDR.

8.3 **IT Manager**:

- Retrieves, corrects, or deletes data from AWS and Entra systems.
- Verifies completion of requests (e.g., deletion confirmation).

8.4 **Customers**:

- Forward end-user requests to Gibble or verify end-user identities.
- Ensure compliance with data subject rights for their data subjects, per the Privacy Policy (Section 3).

8.5 **Employees and Contractors**:

- Report data subject requests received directly to privacy@gibble.com.au.
- Assist the DPO in processing requests, as needed.

9. Documentation and Auditing

9.1 **Documentation**:

- All requests are logged in a secure system, including:
    - Data subject details and request type.
    - Verification and response actions.
    - Outcome and response date.
- Logs are retained for 7 years, per the Data Retention and Deletion Policy (Section 5).

9.2 **Auditing**:

- Quarterly audits verify compliance with response timelines and procedures.
- Annual ISO 27001 and SOC 2 audits include data subject rights processes.
- Audit reports are available to customers upon request at privacy@gibble.com.au.

10. Compliance

10.1 This Policy aligns with:

- GDPR Articles 15-22 (Data Subject Rights).
- APPs 12-13 (Access and Correction).
- IPPs 6-7 (Access and Correction).
- PDPA, CCPA/CPRA, and APPI data subject rights provisions.
- ISO 27001 A.18.1.4 (Privacy and Protection of Personally Identifiable Information).

10.2 AWS and Entra compliance dashboards, supported by Adlumin MDR logs, ensure regulatory adherence.

11. Exceptions and Appeals

11.1 **Exceptions**:

- Requests may be refused if:
    - Identity cannot be verified.
    - The request is unfounded, excessive, or repetitive (GDPR Article 12).
    - Legal obligations (e.g., tax retention) prevent compliance.
- Exceptions are documented and communicated with reasons.

11.2 **Appeals**:

- Data subjects can appeal refusals by contacting the DPO at privacy@gibble.com.au.
- Appeals are reviewed within 14 days, with escalation to regulators if unresolved.

12. Contact Information

12.1 For data subject requests or inquiries, contact:

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

12.2 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.