Privacy by Design and Default 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) Privacy by Design and Default Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Privacy by Design and Default Policy

Last updated: July 2025

1. Purpose

1.1 This Privacy by Design and Default Policy ("Policy") outlines how Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), embeds privacy principles into the design, development, and operation of our SaaS platforms for learning, payroll, student management, and human resources management. The Policy ensures that personal information, customer data, and sensitive data, such as biometric data, are protected by default and throughout the data lifecycle.

1.2 The Policy integrates with our Privacy Policy (Sections 3, 4, 14), Security Policy (Section 4), Data Subject Rights Policy (Section 4), and other policies, leveraging Amazon Web Services (AWS), Microsoft Entra, and Adlumin Managed Detection and Response (MDR) services to implement privacy-focused measures.

1.3 We are committed to compliance with applicable data protection laws, including:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly APP 1.
- EU General Data Protection Regulation 2016/679 (GDPR), Article 25.
- *Privacy Act 2020* (New Zealand), Information Privacy Principle (IPP) 1.
- 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, technology, or business operations. Updates are posted at www.gibble.com.au/privacy-by-design.

2. Scope

2.1 This Policy applies to:

- All Gibble platforms, systems, and infrastructure, including those hosted on AWS (e.g., S3, RDS, EC2), Microsoft Entra (e.g., Azure Blob Storage, Entra ID), and third-party systems (e.g., Salesforce, Stripe).
- Personal information processed by Gibble, including names, contact details, biometric data, payroll records, student data, and analytics data, as described in the Privacy Policy (Section 4).
- All stages of the data lifecycle, from collection to deletion, across Gibble's operations in Australia, New Zealand, the EU, UK, Singapore, USA, and Japan.
- All personnel, including employees, contractors (e.g., in Vietnam and the Philippines for Gibble platforms), vendors, and customers.

2.2 It complements the Privacy Policy (Section 3), Security Policy (Section 4), Data Subject Rights Policy (Section 4), and other policies to ensure a privacy-centric approach.

3. Definitions

3.1 **Privacy by Design**: The proactive integration of privacy principles into the design and operation of systems, processes, and services to protect personal information.

3.2 **Privacy by Default**: Ensuring that the default settings of systems and services prioritise privacy, requiring minimal user intervention to protect personal information.

3.3 **Personal Information**: Information relating to an identified or identifiable individual, as defined in the Privacy Policy (Section 4).

3.4 **Data Minimisation**: Collecting and processing only the personal information necessary for a specific purpose.

4. 4. Privacy by Design and Default Principles

4.1 **Proactive Approach**: Identify and mitigate privacy risks before they occur, integrating privacy into system design and development.

4.2 **Privacy as Default**: Configure systems to protect personal information automatically, without requiring user action.

4.3 **Data Minimisation**: Collect, process, and retain only the data necessary for the intended purpose.

4.4 **Transparency**: Clearly communicate data processing practices to data subjects, per the Privacy Policy (Section 3).

4.5 **User-Centric**: Empower data subjects to exercise their rights (e.g., access, deletion), per the Data Subject Rights Policy (Section 4).

4.6 **End-to-End Security**: Protect data throughout its lifecycle with encryption and access controls, per the Encryption Policy (Section 5) and Access Control Policy (Section 5).

4.7 **Compliance**: Align with GDPR Article 25, APP 1, and other data protection laws.

5. Implementation of Privacy by Design

5.1 **System Design**:

- Privacy requirements are integrated into the Software Development Lifecycle (SDLC) for Gibble's platforms, including Gibble platforms developed by contractors in Vietnam and the Philippines.
- Data Protection Impact Assessments (DPIAs) are conducted for new systems or significant changes processing sensitive data (e.g., biometric data), per GDPR Article 35 and APP 1.

- Systems use role-based access control (RBAC) and multi-factor authentication (MFA) via AWS IAM and Entra ID, per the Access Control Policy (Section 5).

5.2 **Data Minimisation**:

- Collect only necessary personal information, as defined in customer contracts and the Privacy Policy (Section 4).
- Avoid collecting sensitive data (e.g., biometric data) unless explicitly required and consented to, per the Privacy Policy (Section 19.2).
- Anonymise or pseudonymise analytics data where possible, per the Privacy Policy (Section 7).

5.3 **Secure Architecture**:

- Use AES-256 encryption for data at rest and TLS 1.3 for data in transit, per the Encryption Policy (Section 5).
- Implement secure APIs with OAuth 2.0 and encrypted keys via AWS API Gateway.
- Use secure enclaves (e.g., AWS Nitro Enclaves) for processing sensitive data.

5.4 **Change Management**:

- Privacy is considered during system changes, with DPIAs conducted for significant updates, per the Change Management Policy (Section 5).
- Changes are tested in non-production environments to ensure privacy controls remain effective.

6. Implementation of Privacy by Default

6.1 **Default Settings**:

- Platform settings default to the highest privacy protections, requiring user opt-in for non-essential data processing (e.g., analytics, marketing).
- Cookies are disabled by default except for strictly necessary ones, per the Cookie Policy (Section 5).
- Location-based services in the Ready People App require explicit consent, per the Privacy Policy (Section 19.1).

6.2 **User Controls**:

- Data subjects can easily access, correct, or delete their data via the customer or directly through www.gibble.com.au/rights, per the Data Subject Rights Policy (Section 5).
- Consent management tools allow users to modify preferences for data processing.

6.3 **Data Retention**:

- Data is retained only for the minimum period necessary, per the Data Retention and Deletion Policy (Section 5).
- Automated deletion processes ensure data is removed when no longer needed, per the Data Subject Rights Policy (Section 6.3).

7. Security Measures

7.1 **Encryption**:

- All personal information is encrypted using AES-256 for data at rest and TLS 1.3 for data in transit, per the Encryption Policy (Section 5).
- Encryption keys are managed securely via AWS KMS and Azure Key Vault.

7.2 **Access Controls**:

- Access to personal information is restricted to authorised personnel via RBAC and MFA, per the Access Control Policy (Section 5).
- Adlumin MDR monitors access to detect unauthorised attempts, per the Information Security Incident Management Policy (Section 6).

7.3 **Incident Management**:

- Privacy breaches are managed per the Data Breach Response Plan (Section 5) and Information Security Incident Management Policy (Section 8).
- Adlumin MDR provides real-time alerts for privacy-related incidents.

8. Monitoring and Auditing

8.1 **Monitoring**:

- Adlumin MDR monitors systems for compliance with privacy settings and data protection controls.
- AWS CloudTrail and Microsoft Defender for Cloud log data processing activities, per the Access Control Policy (Section 8).

8.2 **Auditing**:

- Quarterly audits verify adherence to Privacy by Design and Default principles.
- Annual ISO 27001 and SOC 2 Type II audits include privacy controls, per the Security Policy (Section 6).
- DPIA outcomes and compliance reports are available to customers upon request at privacy@gibble.com.au.

9. Roles and Responsibilities

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

- Oversees implementation of Privacy by Design and Default principles.
- Conducts DPIAs and ensures compliance with data protection laws.
- Handles data subject inquiries (privacy@gibble.com.au).

9.2 **Security Officer**:

- Ensures privacy controls are integrated into security measures.
- Monitors systems via Adlumin MDR for privacy violations.
- Supports DPIAs for security-related changes.

9.3 **IT Manager**:

- Configures systems to enforce privacy by default settings.
- Implements encryption and access controls for new systems or changes.
- Verifies privacy controls during testing, per the Change Management Policy (Section 5).

9.4 **Employees and Contractors**:

- Adhere to privacy policies during system development and operations, per the Employee and Contractor Security Policy (Section 5).
- Report privacy concerns to privacy@gibble.com.au within 1 hour.

9.5 **Vendors**:

- Comply with Privacy by Design requirements in Data Protection Agreements (DPAs), per the Vendor Management Policy (Section 5).
- Implement privacy controls for systems processing Gibble's data.

10. Training

10.1 Employees and contractors, including those in Vietnam and the Philippines, receive annual training on:

- Privacy by Design and Default principles.
- Conducting DPIAs and assessing privacy risks.
- Handling personal information securely, per the Employee and Contractor Security Policy (Section 7).

10.2 Customers receive guidance on privacy controls during onboarding, per the Acceptable Use Policy (Section 5).

11. Compliance

11.1 This Policy aligns with:

- GDPR Article 25 (Data Protection by Design and by Default).
- APP 1 (Open and Transparent Management of Personal Information).
- IPP 1 (Purpose and Collection).

- ISO 27001 A.18.1.4 (Privacy and Protection of Personally Identifiable Information).
- PDPA, CCPA/CPRA, and APPI privacy requirements.

11.2 AWS and Entra compliance dashboards, supported by Adlumin MDR logs, ensure adherence to these standards.

12. Violations

12.1 Violations of this Policy (e.g., bypassing privacy controls, failing to conduct DPIAs) may result in:

- Disciplinary action for employees or contractors, per the Employee and Contractor Security Policy (Section 12).
- Immediate suspension of access, per the Access Control Policy (Section 12).
- Contractual penalties for vendors, per the Vendor Management Policy (Section 12).
- Reporting to regulators if the violation constitutes a data breach, per the Data Breach Response Plan (Section 8).

12.2 Violations are investigated by the DPO and Security Officer with Adlumin MDR support.

13. Contact Information

13.1 For privacy-related inquiries or to report violations, 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.