

Privacy Policy

Gibble SaaS Platform

Prepared by: Steven Kirkilis, Gregory Ibbotson & Bradley Smith

Version: 1.2



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 Policy

Last updated: July 2025

Table of Contents

1	About this Privacy Policy	3
2	Our Online Platforms	3
3	Customer Responsibility for Data Subject Privacy	3
4	Types of Personal Information We Collect and Hold	4
5	How We Collect Personal Information	4
6	How We Use Personal Information	4
7	Analytics Data	5
8	Location Services Data	5
9	How We Hold and Secure Personal Information	5
10	Disclosure of Personal Information	6
11	Third-Party Websites	6
12	Interacting Without Disclosing Personal Information	6
13	Offshore Disclosure	6
14	Access and Correction of Personal Information	6
15	Complaints	7
16	New Zealand Customers and Data Subjects	7
17	European Customers and Data Subjects	7
18	Other Regions (Singapore, USA, Japan)	8
19	Leftorium Pty Ltd (Gibble) Personnel	8

Leftorium Pty Ltd (Trading as Gibble) Privacy Policy

Last updated: July 2025

1 About this Privacy Policy

1.1 This Privacy Policy outlines how Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), collects, uses, stores, discloses, and protects personal information about our corporate customers, their personnel, end users, and other individuals ("data subjects") whose data is processed via our online platforms. It applies to all Gibble services, including learning, payroll, student management, and human resources management platforms.

1.2 We are committed to complying with all applicable data protection laws, including the Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), the EU General Data Protection Regulation 2016/679 (GDPR) for European data subjects, and the *Privacy Act 2020* for New Zealand data subjects.

1.3 Specific details for customers and data subjects in New Zealand, the European Union, Singapore, the USA, and Japan are provided in dedicated sections below. Information about how we manage personal information of our employees and contractors is also included.

1.4 For inquiries, contact our Privacy Representative and Data Protection Officer 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 We review and update this Privacy Policy periodically. Changes will be posted on our website at www.gibble.com.au/privacy. Significant updates will be communicated via email, website banners, or platform notifications.

2 Our Online Platforms

2.1 Leftorium Pty Ltd, trading as Gibble, owns and operates cloud-based SaaS platforms for learning, payroll, student management, human resources, and related services. Our corporate customers subscribe to or license these platforms under contractual agreements.

2.2 Platform functionality varies based on the specific platform and customer contract, enabling customers to collect, process, and disclose personal information about their end users and data subjects.

2.3 We do not contract directly with data subjects or end users. Our customers are responsible for ensuring compliance with privacy laws when using our platforms.

3 Customer Responsibility for Data Subject Privacy

3.1 Customers must comply with all applicable privacy laws, including obtaining necessary consents and authorisations from data subjects for us to collect, process, and disclose their personal information as per our contracts.

3.2 We rely on customers to ensure that personal information entered into our platforms is accurate, up-to-date, complete, relevant, and not misleading.

3.3 Customers are encouraged to inform their data subjects about their privacy policies, explaining how personal information is collected, used, and processed via our platforms or otherwise.

Leftorium Pty Ltd (Trading as Gibble) Privacy Policy

Last updated: July 2025

4 Types of Personal Information We Collect and Hold

4.1 We collect and hold the following types of personal information:

1. **Content Entered into Platforms:** Information entered by customers or end users, including names, contact details (e.g., email, phone), employment details, payroll data, student records, and biometric data (where applicable, e.g., for time tracking). This may include sensitive information such as health or financial data, depending on the platform's purpose.
2. **Customer Personnel Information:** Names, contact details, billing information (e.g., last four digits of credit card numbers), and job roles of customer personnel. Full credit card details are processed and stored securely by third-party payment gateway providers (e.g., Stripe) and are not accessible by us.
3. **Support, Maintenance, and Security Data:** IP addresses, email addresses, user access logs, usernames, passwords, support ticket details, and error messages to ensure platform functionality and security.
4. **Analytics Data:** De-identified data about platform usage, such as user location, device information, time spent on platforms, and navigation paths (see Section 7).
5. **Location Services Data:** Geolocation data (latitude and longitude) collected with user consent via our mobile apps (e.g., Ready People App) to provide location-based services.

5 How We Collect Personal Information

5.1 We collect personal information only through lawful and non-intrusive means, in compliance with applicable data protection laws.

5.2 **Prospective Customers:** We collect information from public and private databases, marketing events, or voluntarily disclosed information to promote our services.

5.3 **Customers and Data Subjects:** After a customer enters a contract, we collect personal information via:

1. End users entering data directly into our platforms.
2. Customers providing data for migration (e.g., from legacy databases).
3. Third parties (e.g., government agencies) providing data on behalf of customers, as per contractual agreements.
4. APIs transmitting data to our platforms under customer contracts.
5. Voluntary disclosures via email, phone, or online forms.

6 How We Use Personal Information

6.1 The following table outlines how we use personal information and our legal basis for processing:

Category	How We Use and Process Personal Information	Legal Basis
Prospective Customer Personnel	Inform, market, and promote services; negotiate contracts.	Legitimate interests (business operations and growth).
Customer Personnel	Set up, configure, and host platforms; communicate about platform usage; provide technical support, training, and professional services; send billing notices; discuss security	Legitimate interests (business operations, platform delivery);

Leftorium Pty Ltd (Trading as Gibble) Privacy Policy

Last updated: July 2025

Category	How We Use and Process Personal Information	Legal Basis
	requirements; offer promotional materials; administer contracts.	performance of contracts; legal obligations.
Data Subjects	Provide and support platform functionality; migrate data; store data in third-party hosting environments; provide technical support; perform backups, restores, security audits, and incident investigations.	Performance of contracts with customers; legitimate interests (platform and IT system management); legal obligations.

6.2 We process sensitive information (e.g., biometric or health data) only with explicit consent or as required by customer contracts and applicable laws.

7 Analytics Data

7.1 We collect de-identified analytics data (e.g., user location, device type, time spent on platforms) to improve platform performance and develop marketing materials. This data cannot reasonably identify individuals.

7.2 We use Google Analytics for platform analytics. For details, visit [Google's Privacy Policy](#).

7.3 Our platforms use cookies to enhance user experience. For more information, see our Cookie Policy at www.gibble.com.au/cookies.

8 Location Services Data

8.1 With explicit user consent, our platforms and mobile apps (e.g., Ready People App) collect geolocation data (e.g., GPS coordinates) to provide location-based services. Users can disable location tracking via device or app settings.

9 How We Hold and Secure Personal Information

9.1 Personal information is stored in:

1. Our offices and on-premises systems in Australia.
2. Third-party cloud hosting facilities (e.g., AWS, Microsoft Azure) in Australia, New Zealand, Canada, the UK, Singapore, USA, and Japan.
3. Cloud-based CRM and email platforms (e.g., Salesforce, Microsoft 365).
4. Hard-copy files in secure office premises.

9.2 We implement robust security measures aligned with ISO 27001, including:

1. AES-256 encryption for data at rest and TLS 1.3 for data in transit.
2. Role-based access controls and multi-factor authentication (MFA).
3. Regular penetration testing and vulnerability assessments.
4. Firewalls, intrusion detection systems, and endpoint protection.
5. Physical security (e.g., biometric locks, surveillance, secure shredding for hard-copy data).
6. Data Breach Response Plan compliant with APP 11 and GDPR Article 33.
7. Regular employee training on data protection and cybersecurity.
8. Secure data destruction processes for obsolete data.

9.3 We engage reputable third-party hosting providers with ISO 27001 or SOC 2 certifications to ensure data security.

10 Disclosure of Personal Information

10.1 We disclose personal information only as follows:

1. To third parties as required by customer contracts (e.g., data transfers to customer systems or third-party platforms).
2. To hosting providers for database management.
3. To cloud-based platforms (e.g., CRM, payment gateways) for business operations.
4. To contractors (e.g., for software development or support) under strict confidentiality agreements.
5. To legal, financial, or insurance advisors for compliance or dispute resolution.
6. With explicit consent or to protect vital interests (e.g., safety).
7. For law enforcement, public revenue protection, or legal proceedings, as required by law.

10.2 Customers using our platforms to disclose data to third parties must ensure compliance with applicable laws.

11 Third-Party Websites

11.1 Our platforms may link to third-party websites. We do not endorse these sites or guarantee their compliance with data protection laws. Users should review third-party privacy policies before sharing personal information.

12 Interacting Without Disclosing Personal Information

12.1 Users can browse our public website (www.gibble.com.au) without providing personal information. However, platform access, contract initiation, or support services require personal information for identification and service delivery.

12.2 Individuals may use pseudonyms when inquiring about our services, but accurate identification is required for platform account creation and access.

13 Offshore Disclosure

13.1 Personal information may be transferred to third-party service providers in New Zealand, Canada, the UK, Singapore, USA, and Japan for hosting, support, or development purposes. We ensure compliance with APP 8 and GDPR Chapter V through:

- Standard Contractual Clauses (SCCs) for GDPR-covered data.
- Binding corporate rules for intra-group transfers.
- Agreements ensuring equivalent data protection standards.

13.2 For Gibble platforms, contractors in Vietnam and the Philippines may access systems under strict confidentiality agreements.

14 Access and Correction of Personal Information

14.1 End users can update or delete their platform accounts where functionality permits or by contacting the relevant customer. Data may be retained post-deletion as required by customer contracts or legal obligations (e.g., tax records under Australian law).

Leftorium Pty Ltd (Trading as Gibble) Privacy Policy

Last updated: July 2025

14.2 Data subjects seeking access or correction should first contact the customer responsible for their data. Alternatively, they may contact our Privacy Representative at privacy@gibble.com.au.

14.3 We handle access requests within 30 days (or 20 working days for New Zealand data subjects) and may charge a reasonable fee unless prohibited by law. Requests may be refused under applicable legal grounds, with reasons provided.

15 Complaints

15.1 To raise a privacy concern, contact our Privacy Representative at privacy@gibble.com.au. We aim to resolve complaints collaboratively within 30 days.

15.2 If unresolved, complaints can be escalated to:

- **Australia:** Office of the Australian Information Commissioner (OAIC), enquiries@oaic.gov.au, 1300 363 992, GPO Box 5218, Sydney NSW 2001.
- **New Zealand:** Office of the Privacy Commissioner, enquiries@privacy.org.nz, PO Box 10-094, Wellington 6143.
- **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 for CCPA).
- **Japan:** Personal Information Protection Commission, info@ppc.go.jp.

16 New Zealand Customers and Data Subjects

16.1 This section applies to personal information governed by the *Privacy Act 2020* (New Zealand).

16.2 Collection: We collect personal information only for lawful purposes connected to our business functions and do not treat unsolicited information as collected under IPPs 1–4. Unsolicited data receives equivalent security protections.

16.3 Disclosure: We ensure third parties receiving personal information comply with IPPs to prevent unauthorised use or disclosure.

16.4 Access and Correction: Individuals may request confirmation of held data, access, or correction. We respond within 20 working days and may charge a reasonable fee. Refusals are explained, with options to escalate to the Privacy Commissioner.

17 European Customers and Data Subjects

17.1 This section applies to personal data governed by the GDPR.

17.2 Collection: Customers are responsible for obtaining consents for data collection. We process data as per Section 5 and do not collect data from public sources.

17.3 Legal Basis: See Section 6.1 for processing purposes and legal bases (e.g., contract performance, legitimate interests).

17.4 International Transfers: Data transfers to New Zealand, Canada, the UK, Singapore, USA, and Japan comply with GDPR Chapter V via SCCs or adequacy decisions.

17.5 Retention: Data is retained only as long as necessary for the purposes outlined or as required by law, then deleted or anonymised.

Leftorium Pty Ltd (Trading as Gibble) Privacy Policy

Last updated: July 2025

17.6 Rights: Data subjects have rights to information, access, rectification, erasure, restriction, portability, and objection. Contact customers first or our Privacy Representative to exercise these rights.

17.7 Automated Decision-Making: Some platforms use automated decision-making as specified in customer contracts. Data subjects can request details from their customer.

18 Other Regions (Singapore, USA, Japan)

18.1 For customers and data subjects in Singapore (PDPA), the USA (e.g., CCPA/CPRA), and Japan (APPI), we comply with local data protection laws, including:

- Obtaining consents where required.
- Providing rights to access, correct, or delete data.
- Ensuring secure data transfers with appropriate safeguards.

18.2 Contact our Privacy Representative for region-specific details.

19 Leftorium Pty Ltd (Gibble) Personnel

19.1 This section applies to employees and contractors of Leftorium Pty Ltd, trading as Gibble.

19.2 Collection: We collect names, contact details, ABNs, employment history, qualifications, bank details, tax file numbers, superannuation details, identification documents, medical information, and biometric data (e.g., fingerprints for time tracking in some subsidiaries, with explicit consent).

19.3 Use: Data is used for recruitment, employment management, contract administration, and legal compliance (e.g., taxation, superannuation).

19.4 Disclosure: We disclose personnel data to:

1. Next of kin in emergencies.
2. Law enforcement for background checks.
3. Professional referees during recruitment.
4. The Australian Taxation Office or superannuation funds.
5. Third parties as per Section 10 (e.g., hosting providers, legal advisors).

19.5 Security: Personnel data is secured as per Section 9, with access restricted to authorised HR personnel.