



SUPERWORKERTM

PRIVACY POLICY

This policy describes how Superworker collects, uses, discloses, and protects personal information across the website and the Superworker platform. It explains data categories, purposes of processing, international transfers, security measures, and data subject rights. It is intended to be read alongside the EULA and any Data processing Addendum (DPA) or Order Form and does not amend those terms. By using the Service, you agree to the collection and use of information in accordance with this Privacy Policy.

INTERPRETATION AND DEFINITIONS

The words whose initial letter is capitalised have meanings defined below. The following definitions have the same meaning whether they appear in singular or plural.

DEFINITIONS

- **Account** means a unique account created for you to access our Service.
- **Company** refers to Superworker.
- **Cookies** are small files placed on your device that store details of your browsing history on our website, among other uses.
- **Country** refers to the Republic of South Africa, unless your contract specifies another jurisdiction.
- **Device** means any device that can access the Service, such as a computer, a mobile phone, or a tablet.
- **Personal Information** means information relating to an identifiable natural person and, where applicable, a juristic person, including as defined in POPIA and GDPR.
- **Service** refers to the websites at www.superworker.co and the Superworker software-as-a-service platform, including integrations and support.
- **Service Providers** means third-party companies or individuals that facilitate the Service, provide services on our behalf, or assist us in analysing how the Service is used.
- **Usage Data** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, page visits, telemetry, and diagnostics).



info@superworker.co



410 Lynnwood Road,
Lynnwood,
Pretoria,
0081

COLLECTING AND USING YOUR PERSONAL INFORMATION

TYPES OF DATA COLLECTED

Account Data | name, email address, role, authentication identifiers, and tenant membership.

Profile and Organisation Data | team, department, supervisor or manager relationships, locations, and language preferences where configured by your organisation.

Content and Learning Data | learning objects, assignments, completions, assessments, feedback, messages, and related metadata that your organisation chooses to store or connect.

Productivity and Journey Data | sequencing, nudges, checklists, task status, timestamps, and proof-of-completion signals that indicate progress in the platform.

Usage and Telemetry Data | log records, device and browser metadata, performance metrics, and event data used to operate and secure the Service.

Support Data | support tickets and any screen captures or diagnostics you share with us for troubleshooting.

Integration and Directory Data | identifiers and attributes received from connected systems (for example, your HRIS, LMS or LXP, Microsoft 365, or identity provider) to enable single sign-on and orchestration.

Cookies and Similar Technologies | we use cookies and similar technologies to provide the website, remember preferences, and improve the Service. You can control cookies through your browser settings.

****Where required by law, your organisation (as Controller or Responsible Party) ensures a lawful basis for processing. Avoid uploading special-category data unless strictly necessary and authorised.***

USE OF YOUR PERSONAL INFORMATION

- Provide, maintain, and improve the Service, including orchestration features, analytics, and support.
- Authenticate users, enable single sign-on, and enforce security controls.
- Operate integrations with systems you choose to connect.
- Monitor, detect, and prevent security incidents, fraud, or misuse.
- Comply with legal obligations and enforce our terms.
- Communicate about updates, security notices, and service-related messages.

AI-POWERED FEATURES

Where AI features are enabled by your organisation and a large language model (LLM) provider is configured (for example, an OpenAI GPT-class model), we apply data minimisation and safeguards.

- Limit prompts to necessary context and authorised sources. Exclude unnecessary fields.
- Redact direct identifiers from free text where feasible and use tenant-local pseudonyms when correlation is needed.
- Prefer provider options that disable training on customer inputs and outputs and that limit retention where such controls exist.
- Transmit over TLS and retain minimal logs for troubleshooting and abuse detection.



RETENTION OF YOUR PERSONAL INFORMATION

We retain personal information for as long as needed to provide the Service and as required by law, security, or dispute resolution. Your organisation may define retention settings. We follow those instructions.

INTERNATIONAL TRANSFERS AND HOSTING

We host on Microsoft Azure in a region selected by your organisation. If transfers outside that region are required, appropriate safeguards (such as EU Standard Contractual Clauses and the UK IDTA or Addendum) are applied and documented in your DPA or equivalent contract.

YOUR RIGHTS AND CHOICES

Subject to applicable law, including POPIA and GDPR, you may request access, correction, deletion, restriction, portability, or object to processing. Requests should be directed to your organisation. You may also contact us using the details below for assistance within the scope of our role as a Processor or Operator.

DISCLOSURE OF YOUR PERSONAL INFORMATION

We may disclose information to service providers who process data on our behalf, under contract and subject to security and confidentiality obligations.

We may disclose information where required by law or to protect rights, property, or safety, including in connection with a merger, acquisition, or sale of assets.

SECURITY OF YOUR PERSONAL INFORMATION

We apply layered security controls proportionate to risk, including encryption in transit and at rest, role-based access control, single sign-on, monitoring, and backups and disaster recovery. No method of transmission or storage is 100% secure.

CHILDREN'S PRIVACY

The Service is not directed to children. If you believe a child's personal information has been provided without proper authority, please contact us so we can take appropriate steps.

LINKS TO OTHER WEBSITES

Our websites may contain links to other sites. We have no control over, and assume no responsibility for, the content, privacy policies, or practices of any third-party sites or services.

CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time. We will post the new policy on this page and, where appropriate, notify administrators through the Service.