SUPERWORKER

ASSURANCE ATTESTATIONS PACK

This document provides a concise overview of how Superworker operates in practice. It outlines our approach to data processing, security, incident response, supplier reliance, and geographic data handling. The goal is to support due diligence by showing the controls in place and the certified cloud infrastructure we use. It does not change any agreement. If there is any conflict, the EULA and any signed Order Form or Data Processing Addendum (DPA) take precedence. Use this document to understand responsibilities between customer and provider, where evidence can be found, and how we align day to day operations with accepted security and privacy practices.

PURPOSE AND PRECEDENCE

PURPOSE | Concise, accurate description of controls and supplier certifications that support your compliance posture.

SCOPE | Superworker SaaS platform and related support channels.

PRECEDENCE | Informational only. Contractual terms are defined in the EULA and, where applicable, a DPA or Order Form.

SHARED RESPONSIBILITY | The customer retains responsibility for lawful basis, configuration, user lifecycle, and integration governance.

DATA PROCESSING (ATTESTATION)

Superworker processes personal data solely to deliver and support the service, on the documented instructions of the customer (Controller or Responsible Party). Where applicable, Superworker acts as Processor or Operator. We minimise data collection and keep account, usage, content, and support data categories distinct.

- Lawful instructions only. No processing beyond documented purposes.
- No sale of personal data. No training of public models on customer content.
- International transfers use appropriate safeguards (for example, SCCs or the UK IDTA) and are documented in the DPA or Evidence Pack.
- Deletion or return of data at termination per contract, except where law requires retention.

** **Reference documents kept separate: Privacy Policy; Data Processing Addendum (on request).***

SUBPROCESSORS (ATTESTATION)

Subprocessors provide infrastructure or features under contract. Superworker remains responsible for their performance and flows down equivalent obligations via written agreements.

- Supplier example: Microsoft Azure (compute, storage, networking). ISO/IEC 27001, 27017, 27018 certified. See Microsoft Trust Center or Service Trust Portal.

info@superworker.co

410 Lynnwood Road,
Lynnwood,
Pretoria,
0081

- Optional providers may include identity (SSO), notifications, observability, and AI model providers, as configured per tenant.
- Changes to subprocessors are notified per contract. Customers may raise reasonable objections where applicable.

**** Reference document: Subprocessors List (maintained; latest provided in the Evidence Pack).***

DATA FLOW AND RESIDENCY (ATTESTATION)

Customers select a primary Azure region. Application, storage, and backups are provisioned within that region by default. Where cross-border transfers are required, we document the flow, apply safeguards, and obtain customer authorisation.

USER AUTHENTICATION | The identity provider validates credentials (customer SSO or Superworker) and issues tokens.

APPLICATION USE | Requests reach Azure services. Content and telemetry are written to region-bound storage and logs.

INTEGRATIONS | Connectors exchange metadata via secure APIs with least-privilege scopes and auditable tokens.

NOTIFICATIONS | Email and SMS providers process minimal metadata to deliver messages.

SUPPORT | Tickets and diagnostics are stored with restricted access and time-bound retention.

**** Reference document: Data Flow and Residency Summary.***

SECURITY OVERVIEW (ATTESTATION)

Superworker operates on Microsoft Azure and implements layered controls focused on access, data, change, and recovery. We align to commonly accepted security practices, and we do not claim our own ISO certifications.

ENCRYPTION | TLS in transit; industry-standard encryption at rest.

ACCESS | Role-based access control (RBAC), SSO and MFA support, least-privilege administration, periodic access reviews.

LOGGING AND MONITORING | Centralised logs, alerting, and audit trails for administrative activity.

BACKUPS AND DR | Automated backups with periodic restore tests. Documented RPO and RTO targets supplied on request.

SECURE DEVELOPMENT | Threat modelling, code review, dependency scanning, and periodic third-party testing.

CHANGE CONTROL | Ticketed changes with approvals and rollback plans.

Supplier certifications (Microsoft Azure): ISO/IEC 27001, 27017, 27018. See Microsoft Trust Center or Service Trust Portal.

**** Reference documents: Security Overview; Incident Response Summary.***

INCIDENT RESPONSE (ATTESTATION)

We maintain an incident management process designed to restore service quickly, minimise impact, and meet legal obligations. This includes severity classification (SEV1 to SEV4), an incident commander, containment, eradication and recovery steps, and post-incident reviews. Breach notifications are made without undue delay after becoming aware, subject to investigation.

- A single ticket of record with documented handoffs and notes. Executive escalation path where applicable.
- Regulatory notifications are coordinated with the customer where required by law.

**** Reference document: Incident Response Summary.***

COMPLIANCE MATTERS (ATTESTATION)

Superworker is not ISO-certified. We operate aligned to these frameworks on certified supplier infrastructure. Supplier certifications support your compliance posture. Your obligations depend on configuration, jurisdiction, and use case.

- **Supplier certifications (examples):** ISO/IEC 27001 (ISMS), 27017 (cloud controls), 27018 (PII in public cloud) for Microsoft Azure.
- **Evidence Pack during diligence:** EULA, Privacy Policy, PAIA Manual, DPA, Subprocessors, Data Flow and Residency, Security Overview, Incident Response Summary.

ANONYMISATION AND PSEUDONYMISATION FOR AI FEATURES (ATTESTATION)

Where AI features are enabled and a large language model (LLM) provider is configured (for example, OpenAI GPT-5 or another customer-selected provider), Superworker applies controls to minimise personal data exposure and to respect provider options that limit data use.

- **Data minimisation:** Prompts include only what is necessary. Unnecessary fields are excluded.
- **Direct-identifier redaction:** Emails, phone numbers, employee IDs, and similar identifiers are masked or removed where feasible.
- **Pseudonymisation:** Identifiers are replaced with tenant-local pseudonyms or hashed surrogates when correlation is required.
- **Free-text safeguards:** Pattern-based redaction and optional entity masking reduce accidental disclosure in unstructured text.
- **Context scoping:** Retrieval is limited to authorised, relevant documents. Bounded request windows prevent over-sharing.
- **Provider configuration:** Where available, options are selected to prevent use of inputs or outputs for public model training and to limit retention.
- **Transport security:** Model requests are sent over TLS. Responses are logged with minimised metadata for troubleshooting.
- **Customer responsibilities:** Avoid unnecessary personal or special-category data in prompts. Apply DLP or classification. Review outputs before action.

**** Note: Provider-specific behaviours, such as retention and training, are governed by provider terms and tenant configuration. Customers may request current settings.***

SUPPLIER REFERENCES

Microsoft Trust Center (Compliance and Security): https://learn.microsoft.com/azure/compliance/

Microsoft Service Trust Portal (Audit Reports; sign-in required):
https://servicetrust.microsoft.com/

DOCUMENT LINKS (SEPARATE FILES)

- EULA (separate)
- Privacy Policy (separate)
- PAIA Manual (separate)
- EU AI Act Attestation (separate)