SUPERWORKER™

EU AI ACT ATTESTATION

This attestation explains how Superworker aligns with the EU AI Act using a conservative, risk-based approach. It clarifies roles for customers and providers, distinguishes our platform from third-party general-purpose models, and maps relevant duties such as transparency, human oversight, monitoring, and timelines. It is informational and does not amend any agreement. Where there is a conflict, the EULA and any signed Order Form or Data Processing Addendum (DPA) prevail. Use this document to understand how features are categorised against the Act, how prohibited practices are avoided, how GPAI provider responsibilities are treated, and which obligations phase in on specific dates.

1. SCOPE AND ROLES

Superworker provides an orchestration platform that may include AI-assisted features when enabled by the customer. Customers typically act as Controllers or Responsible Parties and Deployers under the AI Act. Superworker acts as a Processor or Operator and, where it offers an AI-enabled feature, as the provider of that feature. Where customers configure a general-purpose model (for example, a GPT-class model), that model's provider remains independently responsible for its own legal obligations under the AI Act.

2. KEY PILLARS OF THE EU AI ACT AND SUPERWORKER'S ALIGNMENT

2.1 RISK-BASED FRAMEWORK

The AI Act applies a graded approach: prohibited practices (unacceptable risk), high-risk systems (stringent obligations), general-purpose AI (GPAI) obligations, limited-risk transparency duties, and minimal-risk uses. Superworker aligns to this structure by classifying features and deployments, avoiding prohibited uses, and supporting customers where a deployment falls into high-risk categories.

2.2 PROHIBITED PRACTICES (ARTICLE 5)

The Act bans certain AI practices, for example manipulative techniques that cause harm, exploitation of vulnerabilities, social scoring, unlawful biometric categorisation, and certain biometric identification uses. Superworker's approach: we design features to avoid prohibited uses, include policy guardrails, and reserve the right to disable features that would contravene Article 5 when configured or used improperly.

info@superworker.co

410 Lynnwood Road,
Lynnwood,
Pretoria,
0081

2.3 GENERAL-PURPOSE AI (GPAI) OBLIGATIONS

Providers of GPAI models must meet transparency and documentation duties, for example technical documentation, a copyright policy, and a summary of training content. Where a GPAI model presents systemic risk, additional measures apply, including risk assessments, incident reporting, cybersecurity, and adversarial testing.

Superworker's approach: when customers configure a third-party GPAI model (for example, an OpenAI GPT-class model), we rely on the model provider to meet its GPAI obligations. We scope prompts and retrieval to the minimum necessary, prefer provider settings that disable public training on customer inputs and outputs where available, and document the model provider and configuration in the tenant Evidence Pack.

2.4 HIGH-RISK AI SYSTEMS (ARTICLES 8–15, ANNEX III)

High-risk systems must implement a risk management system; data and data-governance controls; technical documentation; record-keeping; transparency to deployers; human oversight; and measures for accuracy, robustness, and cybersecurity. Examples can include employment-related uses that may significantly affect individuals, for example automated CV ranking or decisions.

Superworker's approach: we default to assistive AI with human-in-the-loop patterns. Where a customer use case is high risk, we support the customer's obligations by providing configuration documentation, logging, role and permission controls, and evidence of supplier controls (for example, Microsoft Azure certifications). The customer, as Deployer or Controller, remains accountable for DPIAs, lawful basis, oversight, and outcome review.

2.5 LIMITED-RISK TRANSPARENCY

For certain AI interactions, for example chatbots or synthetic content, users must be informed that they are interacting with AI and when content is artificially generated or manipulated.

Superworker's approach: when such features are enabled, we support visible indicators and administrator options for disclosures.

2.6 POST-MARKET MONITORING AND INCIDENT REPORTING

The AI Act requires monitoring of performance and reporting of serious incidents for relevant systems.

Superworker's approach: our incident process supports timely notification to customers, and we expect model providers to meet their own incident obligations. Customers receive logs and summaries required to investigate and meet their regulatory duties.

2.7 CONFORMITY ASSESSMENT AND CE MARKING (HIGH-RISK PROVIDERS)

Providers that place high-risk AI systems on the EU market must follow conformity assessment, maintain a quality management system, and apply CE marking and declarations of conformity.

Superworker's approach: where Superworker is not the provider of a high-risk AI system, we do not seek CE marking. We support customers with documentation of our controls and supplier evidence.

2.8 GOVERNANCE AND ENFORCEMENT

The EU AI Office and national authorities oversee implementation and enforcement. Significant fines apply for non-compliance.

Superworker's approach: we maintain an internal register of AI-enabled features, map use cases to risk categories, and update this attestation as guidance evolves.

3. ANONYMISATION AND PSEUDONYMISATION PROTOCOLS FOR AI FEATURES

When AI features are enabled and a large language model (LLM) provider is configured, Superworker follows a conservative pattern:

- Minimise inputs and exclude unnecessary fields and special-category data.
- Redact direct identifiers in free text where feasible. Use tenant-local pseudonyms when correlation is required.
- Restrict retrieval to authorised sources with bounded context windows.
- Transmit over TLS. Log minimally for troubleshooting and abuse monitoring.
- Prefer provider options that disable training on customer inputs and outputs and that limit retention where available.

Model-specific behaviours, such as retention, follow the model provider's terms and the tenant configuration. Customers should avoid unnecessary personal data in prompts and must review outputs before action.

5. Timelines (Summary)

- Entry into force: 1 August 2024.
- Prohibited practices and AI literacy: from 2 February 2025.
- GPAI obligations: from 2 August 2025, with additional requirements for models presenting systemic risk.
- Broad application: by 2 August 2026, with some high-risk product-embedded systems extended to 2027.

Superworker monitors official guidance and updates this attestation as obligations phase in.

6. CUSTOMER RESPONSIBILITIES (CONTROLLER/DEPLOYER)

Customers determine lawful basis, purpose, and proportionality; conduct impact assessments; configure human oversight; and ensure that uses in employment or other sensitive contexts meet high-risk requirements where applicable. Superworker provides evidence of platform controls and supplier certifications to support these obligations.

7. REFERENCES AND CONTACTS

- EU AI Act: Official Journal (Regulation (EU) 2024/1689).
- EU AI Act: European Commission pages on timelines and GPAI obligations.
- Microsoft Azure: Trust Center and Service Trust Portal (supplier certifications).