

Third-Party (Subprocessor) Management Policy

How Workplacer selects, contracts, and oversees the third-party providers that process customer data.

1. PURPOSE & SCOPE

This policy defines how Workplacer manages the third-party subprocessors that store, transmit, or process data on behalf of the platform — infrastructure, AI, communication, and monitoring providers. It applies to any provider that could access personal data.

2. SELECTION & DUE DILIGENCE

- **EU-first residency** — we default to providers that host data in the EU; primary data (hosting, database, file storage, cache, error monitoring) is EU-resident.
- **Security assurance** — we select established providers that maintain recognised independent security certifications (ISO 27001 / SOC 2) and audited compliance programs, providing third-party assurance of their controls.
- **Purpose fit** — a provider is engaged only where it is necessary to deliver platform functionality.

3. CONTRACTUAL SAFEGUARDS

- Each subprocessor is bound by a Data Processing Agreement incorporating obligations equivalent to those we owe our customers (confidentiality, security, purpose limitation, breach notification, deletion/return of data).
- Transfers of personal data outside the EU are governed by the European Commission's current (2021) Standard Contractual Clauses, incorporated into each provider's DPA.

4. TECHNICAL MEASURES AT THE BOUNDARY

- Encryption in transit (TLS 1.3) and at rest (AES-256).
- Data minimisation — only the data necessary for a provider's function is shared.
- For AI processing, personal data is automatically PII-scrubbed before transmission and is not used to train external models.
- All data access is scoped to the owning company.

5. ONGOING MANAGEMENT

- We maintain a current subprocessor list identifying each provider, its function, and its location.
- Customers are notified of material subprocessor changes, consistent with our Data Processing Agreement.
- Provider security posture and certification status are monitored; a provider that no longer meets our requirements is remediated or replaced.

6. REVIEW

This policy and the subprocessor list are reviewed at least annually and when a subprocessor is added, removed, or materially changed. Formalised periodic vendor risk assessments will be expanded as our compliance program matures.

This policy should be read alongside our Data Processing Agreement (which contains the authoritative subprocessor list) and Information Security Risk Management summary.

Workplacer AI — Third-Party (Subprocessor) Management Policy v1.0. Confidential. Provided in response to security due-diligence requests.