

Privacy by Design — Overview

How Workplacer embeds privacy into its architecture and development, mapped to the seven foundational principles.

OVERVIEW

Workplacer applies privacy-by-design principles throughout its architecture and development process. Privacy is built into how the platform is designed, built, and operated — not added afterwards. The measures below map to the seven foundational principles (Cavoukian).

1. PROACTIVE NOT REACTIVE; PREVENTATIVE NOT REMEDIAL

Privacy risks are prevented in design and code rather than patched afterwards:

- Multi-tenant data isolation is enforced at the data-query layer (not the user interface).
- Automated architecture and security audits run on every code change and flag any query not scoped to the owning company.
- Personal data is scrubbed of PII before it reaches AI processing.
- Every change passes human and AI-assisted security review before deployment.

2. PRIVACY AS THE DEFAULT SETTING

Structural privacy protections are always on and cannot be disabled: per-tenant isolation, encryption in transit and at rest, least-privilege access, and a standing rule that customer personal data is never used to train external AI models. Employee survey responses are collected anonymously by default. Customers can additionally configure how much document content the AI may access — including a PII-redacted mode — or disable AI processing entirely.

3. PRIVACY EMBEDDED INTO DESIGN

Privacy is built into the data model and platform, not bolted on: every record is scoped to a company; access is governed by role-based, capability-level permissions; and a PII-redaction pipeline, a configurable data-retention framework, and GDPR data-export and erasure functions are first-class product features.

4. FULL FUNCTIONALITY — POSITIVE-SUM, NOT ZERO-SUM

Privacy controls do not remove capability. The PII-redacted AI mode still delivers AI analysis; anonymised survey data still yields insight; tenant isolation is invisible to the user experience. Customers gain privacy without giving up functionality.

5. END-TO-END SECURITY — FULL LIFECYCLE PROTECTION

Data is protected across its lifecycle: encryption in transit (TLS 1.3) and at rest (AES-256); secure processing and storage; and secure deletion at end of life — records are hard-deleted with referential cascades, associated files are removed from storage, and audit records are anonymised rather than retained. Deleted data ages out of a 7-day encrypted backup window. All data-changing operations are recorded in an immutable audit log.

6. VISIBILITY AND TRANSPARENCY

Our practices are openly documented: a published Privacy Policy, Data Processing Agreement, subprocessor list, Data Retention Schedule, and AI Governance Policy, plus a public Trust page. Within the product, per-company AI usage is metered and the data-handling mode is visible and configurable by customer administrators.

7. RESPECT FOR USER PRIVACY — KEEP IT USER-CENTRIC

Individuals can export their personal data and request erasure through self-service functionality (GDPR Articles 15, 17, 20); customers control AI data access and can disable it; customers own their data and can extract it during the agreement and for 30 days after termination, after which it is deleted or anonymised.

REVIEW

Privacy-by-design is operated as an embedded practice rather than a separately certified program. This overview is reviewed at least annually and when the platform's data-processing activities change materially.

This document should be read alongside our Privacy Policy, Data Processing Agreement, Data Retention Schedule, and AI Governance Policy.