

Data Retention Schedule

How long Workplacer retains each category of personal and operational data, and how it is deleted.

1. PURPOSE AND PRINCIPLE

Workplacer retains personal data only for as long as necessary to fulfil the purpose for which it was collected, to provide the contracted service, or as required by applicable law. This schedule sets out the retention period for each category of data we process. Two overarching rules govern every category:

- **Account-lifecycle rule.** Data tied to a customer account is retained for the life of the Client Agreement. On termination, Client Data is returned or securely deleted at the Client's choice; Clients may extract their data for **30 days after termination**, after which it is deleted or anonymized (DPA §13).
- **Right to erasure.** Individuals can request deletion at any time via self-service or administrator-initiated erasure. Where records must be preserved for audit or legal reasons, the personal identifiers are **anonymized** rather than retained (user identifier replaced, IP address removed).

2. RETENTION SCHEDULE

Data category	Personal data?	Retention period	Basis / mechanism
Account identity — name, email, login role/membership	Yes	Account lifetime, then deleted or anonymized on termination or erasure request (30-day post-termination extraction window)	Account-lifecycle rule; DPA §13; GDPR erasure endpoints
Authentication sessions	Yes	7 days (expires 7 days after last activity)	Session expiry configuration
Password-reset tokens	Yes	1 hour (single-use)	Token expiry policy
Email-verification / OTP tokens	Yes	1 hour; self-serve signup codes 10 minutes	Token expiry policy
Client Data — sites, contracts, projects, documents, reports, knowledge base	May contain	Account lifetime, then returned or securely deleted on termination (30-day extraction window)	Account-lifecycle rule; DPA §13

Data category	Personal data?	Retention period	Basis / mechanism
Audit / activity logs	Yes (actor identity, IP)	Account lifetime by default; each Client may configure a shorter fixed period (e.g. 90 / 180 / 365 days). Purged nightly against the configured period	Per-company retention setting; daily retention job
In-app notifications	Limited	180 days (default; Client-configurable, minimum 30 days)	Retention framework; nightly sweep
Inbound email (document intake)	May contain	365 days after processing (default; Client-configurable, minimum 90 days)	Retention framework; nightly sweep
Database backups (point-in-time recovery)	Mirror of live data	7 days (rolling window)	Continuous WAL / PITR
AI embeddings (semantic search)	No — PII scrubbed before processing	Life of the source document; contains no direct personal identifiers	Automatic PII redaction before embedding (enforced in production)
Short-lived operational tokens — OAuth state, idempotency keys, mobile handoff, FX cache	Minimal / none	60 seconds – 24 hours depending on token type	Per-feature time-to-live
Shareable links & API credentials — client portal, share links, API keys	Depends on shared content	Customer-controlled expiry (commonly 30–90 days)	Per-object expiry set by the customer

3. DELETION AND ANONYMIZATION MECHANISMS

Mechanism	What it does
Data export	Exports all of an individual's personal data as JSON (GDPR Art. 20)
Self-service erasure	Anonymizes audit logs, then deletes memberships, sessions, accounts, and the user record
Administrator erasure	Erases another user; global identity deleted only when the user belongs to no other Client
Retention sweeps	Nightly scheduled jobs purge audit logs, notifications, and inbound email past their configured periods
Account termination	Client Data returned or securely deleted per DPA §13; 30-day extraction window

4. THIRD-PARTY PROCESSING

Personal data sent to AI providers for analysis and semantic search is minimized and **automatically scrubbed of direct personal identifiers before transmission**. No personal data is used to train external AI models. Sub-processor locations and transfer mechanisms are published in the Data Processing Agreement.

5. NOTES AND EXCEPTIONS

- **Legal hold.** Where retention is required by law (e.g. tax, contractual, or litigation obligations), data may be retained beyond the periods above for the duration of that obligation.
- **Configurable periods.** Categories marked "Client-configurable" default to the values shown; a Client administrator may set a shorter or longer period within the stated bounds.
- **Backups.** Deleted records may persist in the 7-day recovery window until it rolls off; they are not restored into live service except during a documented recovery event.

This schedule is reviewed at least annually and updated when processing activities or retention periods change. It should be read alongside the Privacy Policy (§7 Retention) and the Data Processing Agreement (§13 Deletion or Return of Data).