

Data Retention Schedule

How long each category of data is kept, why, and how it is deleted.

Version 1.4 | Effective 12 August 2026 | Privacy & data

Owner Obedience Global Ltd board | Approved by Obedience Global Ltd board on 12 August 2026

Approval state company-approved | Next review 28 October 2026

01 The schedule

Personal data is kept only as long as its purpose requires:

Data category | Retention | Why

Access-request enquiries | 12 months from last contact | Onboarding conversations span months for practices

Active Quantify account and workspace data | Life of the contract + up to 30 days | Export is offered first; active application records are then deleted, subject to legal holds

Customer project data | Customer-controlled during the contract + up to 30 days after verified termination or deletion instruction | Customers control their commercial record and can request export before deletion

Encrypted database backups | Rolling 30-day cycle after active deletion | Disaster recovery copies age out rather than being restored into active use

Clerk authentication and identity copies | Life of the service + up to 90 days after termination | Current Clerk DPA deletion period; live access is revoked earlier

Security and authentication logs | 12 months | Incident investigation and account protection

ClientID account reference and non-reuse tombstone | Active account life; the retired reference and internal account link are retained after closure to prevent reassignment, subject to periodic legal review | Account continuity, fraud prevention and avoiding one organisation receiving another organisation's former reference

ClientID lookup audit | 12 months unless an active investigation or legal hold requires longer restricted retention | Detecting enumeration, investigating support access and demonstrating accountable use

Billing and tax records | 6 years | HMRC and Companies Act requirements

Current public-assistant provider processing | Not used for model training by default; standard provider API content or abuse-monitoring records may be retained for up to 30 days | Provider legal and safety exceptions may retain limited flagged records for longer; endpoint-specific application state can have a different lifecycle

02 How deletion works

Live application records are deleted from the production database on schedule. Backup copies age out of the rolling backup window within 30 days of active deletion and must not be restored into active use without reapplying the deletion. Authentication-provider copies follow their separate contractual deletion period, currently up to 90 days after termination. Where law, a narrow legal hold or a provider security exception requires longer keeping, only the minimum necessary is retained, isolated and access-restricted.

Canonical online record: <https://obedience.global/policies/data-retention>