RegAlign®

Data Retention and Deletion

Status: Canonical. Issued in the Pilot Pack. Forms part of the DPA on conversion. **Owner:** Sabrina Stewart.

Principle

Customer Personal Data belongs to the Customer. RegAlign retains it only for as long as the Customer instructs, or as long as is necessary to deliver the service plus a defined audit residue.

Default retention windows

Data class	Default retention	Notes
Tenant configuration (obligations, controls, monitoring plans)	Life of contract + 12 months	Restorable on reactivation within 12 months
Compliance evidence (uploads, attestations, test results)	Life of contract + 7 years	Aligns with JFSC handbook expectation; customer may shorten in writing
Audit trail entries (append-only, hash-chained)	Life of contract + 7 years	Cannot be edited; retention extends to preserve chain integrity
Board / regulator pack outputs	Life of contract + 7 years	Restorable to PDF on request after termination
Notifications, digests, system emails	90 days	Email content; metadata persists in audit trail
AI invocation logs (prompt fingerprint, model version, consumer)	24 months	Used for governance and incident review; never used for training
Application logs (technical)	30 days	Operational telemetry only; no customer data fields
Access requests (name, email, firm, role, reason, IP, user-agent)	24 months from submission, or until deletion requested	Captured at `/request-access`; lawful basis: legitimate interests (access control + audit). Deletion on email to `hello@regalign.app`.
Authentication audit (sign-in / sign-out events, IP, user-agent)	~7 days in auth logs	Account profile (name, email, firm) retained while account is active plus a reasonable post-termination audit window.

Customer may override any window downward in writing without invalidating the audit trail. Override upward requires a written instruction citing the legal basis.

Exit and deletion

On termination of contract or pilot:

- 1. **Export window — 30 days.** Customer receives a machine-readable export of all tenant data (Postgres-compatible SQL plus an evidence archive). Export schema is documented and version-stamped.
- 2. **Read-only access — 90 days.** Tenant remains accessible read-only for audit walkbacks and late evidence retrieval.

- 3. **Soft delete — day 90.** Tenant is marked deleted; data remains encrypted at rest and is inaccessible to all users including RegAlign personnel.
- 4. **Hard delete — day 120.** All Customer Personal Data is destroyed from primary storage. Confirmation issued to Customer's DPO.
- 5. **Backup expiry — day 150.** Rolling encrypted backups complete their natural rotation. Final destruction certificate issued.

Audit residue (intentionally retained)

After hard delete, the following non-identifying records are retained for regulatory and contractual defence:

- Append-only audit trail entry stating the deletion event, actor, and timestamp.
- Tenant identifier (UUID only — no name, no contact, no content).
- Hash of the final state for chain integrity.

No Customer Personal Data is retained in this residue.

Customer-initiated deletion of individual records

Where a data subject exercises a right of erasure that the Customer (Controller) is obliged to honour, the Customer may delete the affected record from the tenant. The audit trail records the deletion event (who, when, scope) but not the deleted content. Deletion of a record does not break the chain.

Backups

Backups are encrypted, EU-resident, retained for 30 rolling days, and tested quarterly. Restore is tenant-scoped — a single tenant can be restored without exposing other tenants.

Verification

Customers may request, under NDA: the deletion runbook, the most recent restore test report, and confirmation of destruction at hard-delete date for any terminated tenant.
