

ORamaVR SA**Data Retention Policy***Retention schedule, deletion methods and legal-hold rules for data processed by ORamaVR**Document ID: OVR-POL-014***1. Status, purpose and scope**

1.1 This Data Retention Policy (OVR-POL-014) is an ORamaVR Standard-Form Document, published at oramavr.com/legal/data-retention. It sets out how long ORamaVR retains each category of data it processes in connection with its products and services, and how data is deleted or anonymised at the end of the applicable period. It is referenced by the Standard Contractual Clauses Annex Set (OVR-ADD-SCC-001, Annex I.B) and is read together with the Data Processing Agreement (Exhibit C, OVR-SCH-003), the Information Security & Trust Policy (OVR-POL-007) and the Privacy Policy (OVR-POL-002). Capitalised terms not defined here have the meanings given in the ORamaVR Master Glossary (OVR-GLO-001).

1.2 ORamaVR may update this Policy by publishing a revised version at the URL above; a change that materially shortens a retention protection or materially extends retention of personal data takes effect on not less than thirty (30) days' notice, and any other change on not less than ten (10) days' notice, in accordance with the Standard-Form Document Amendments mechanism in the applicable Principal Agreement. Notices: legal@oramavr.com; data-protection matters: privacy@oramavr.com.

2. Principles

2.1 ORamaVR applies data minimisation and storage limitation: personal data is kept only for as long as needed for the purposes for which it was collected, to perform the applicable agreement, or to comply with legal obligations. Where a business need can be met with aggregated or anonymised data, the identifying data is deleted or anonymised. No patient-identifiable data is intended to be processed on ORamaVR platforms (OVR-SCH-002 §4).

3. Retention schedule

3.1 The following periods apply unless a shorter or longer period is required by law, agreed in the applicable Principal Agreement or Order Form, or expressly configured by the customer within the product:

Data category	Retention period	Notes
Account and tenant data (tenant configuration, administrator and Authorised User accounts)	Term of the Principal Agreement + 90 days	Deleted or anonymised within 90 days of termination or expiry, subject to Section 5.
Training records and analytics (session records, competency reports, learner rosters)	Term + 30-day export window, then deletion within 90 days of termination	Customers may export in a structured, commonly used, machine-readable format during the 30-day window provided under the applicable master agreement; deletion completes within 90 days of termination.
Voice audio (speech-to-text input, in-session audio)	Transient — processed for the session; not retained beyond 30 days	Processed in real time for the live session; any temporary buffers are deleted within 30

Data category	Retention period	Notes
		days unless a longer period is expressly configured by the customer.
Transcripts (JARIA session transcripts, where enabled)	Term of the Principal Agreement	Then deleted or returned per the DPA (OVR-SCH-003 §9).
Billing and tax records	10 years	Swiss Code of Obligations Art. 958f statutory bookkeeping retention.
Support tickets and related correspondence	3 years from closure	Retained for service continuity and defence of claims.
Logs and security telemetry	12 months	Rolling deletion; security-incident artefacts may be preserved longer under Section 6.
Backups	Rolling 35 days	Encrypted backups age out on cycle; data deleted from production is removed from backups as the cycle completes (maximum 35 days).

4. Deletion and anonymisation methods

4.1 At the end of the applicable retention period, data is (a) securely deleted using industry-standard techniques appropriate to the storage medium (logical deletion followed by storage-level erasure or cryptographic erasure of the relevant encryption keys, consistent with recognised standards such as NIST SP 800-88); or (b) irreversibly anonymised so that it no longer relates to an identified or identifiable person, in which case the anonymised data may be retained for statistical and product-improvement purposes.

4.2 Backups. Data deleted from production systems remains in encrypted backups only until the rolling 35-day backup cycle completes, after which it is unrecoverable. Backup media are not used to restore deleted data except as necessary for disaster recovery, in which case deletions are re-applied.

5. Return and deletion under the DPA

5.1 Where ORamaVR processes personal data as processor, the return and deletion provisions of the Data Processing Agreement (OVR-SCH-003 §9) prevail: on termination or expiry of the Principal Agreement, or on the Controller's written request, ORamaVR will at the Controller's election return all personal data in a structured, commonly used, machine-readable format within thirty (30) days, or securely delete and destroy it and confirm deletion in writing within thirty (30) days — subject in each case to the backup cycle in Section 4.2 and the legal-hold exception in Section 6. The 30-day post-termination export window for training records and analytics provided under the applicable master agreement is unaffected.

6. Legal hold

6.1 Retention periods are suspended for data subject to a legal hold — data that ORamaVR is required to preserve for actual or reasonably anticipated litigation, investigation, audit or regulatory proceedings,

or that it must retain under applicable law. Held data is preserved only for as long as, and to the extent, the hold requires, is segregated from ordinary use where practicable, and is deleted per this Policy once the hold is released.

7. Ownership and review

7.1 This Policy is owned by ORamaVR Legal/Compliance with the DPO and is reviewed at least annually and on material changes to products, law or infrastructure. It is governed by Swiss law. Questions: privacy@oramavr.com.