
Exhibit C — Data Processing Agreement

Exhibit C — how ORamaVR processes personal data for its customers

Effective 22 October 2026 · GDPR Art. 28 · Swiss FADP Art. 9 · Replaces v1.3

This Data Processing Agreement (“DPA”) is Exhibit C to, and forms part of, the agreement that incorporates it (the “Principal Agreement”): the OEM Master Agreement, the Direct Master Subscription Agreement, the Master Distribution Agreement, a Custom SIM Service Agreement, the VTC End-Customer Terms (Exhibit B) or any other ORamaVR agreement that refers to Exhibit C. On personal data, this DPA prevails over the Principal Agreement.

One document. This DPA replaces and absorbs the US DPA Addendum — End Customer (OVR-SCH-003-US-EC), the Publisher DP Acknowledgement (OVR-SCH-003-US), the Standard Contractual Clauses Annex Set (OVR-ADD-SCC-001), the Information Security and Trust Policy (OVR-POL-007) and, for customer data, the Data Retention Policy (OVR-POL-014). A reference in any ORamaVR agreement to one of those documents is a reference to the corresponding part of this DPA.

1. SCOPE AND ROLES

1.1 Scope. This DPA applies to personal data processed in connection with the VTC Platform, JARIA, the SIM Library, ORamaVR Creator tenants and related support and services.

1.2 Roles. Personal data that ORamaVR processes on the customer’s behalf is processed with ORamaVR as processor and the customer as controller (Section 5). Personal data that ORamaVR processes for its own purposes — accounts and contracts, billing, security of its services, service data and aggregated statistics — is processed by ORamaVR as an independent controller under its Privacy Policy (Section 4). Where an Authorized Channel Partner administers a customer’s tenant, it acts as ORamaVR’s sub-processor (Section 5.6). Publishers receive only statistics aggregated across at least five customer organisations, which contain no personal data; they are not parties to this DPA.

1.3 JARIA. Personal data processed through JARIA — voice audio, transcripts, prompts, outputs and session context — is processed by ORamaVR as processor under Section 5, like any other customer data. Annex J to the JARIA Terms of Use (the JARIA Addendum) adds the AI-specific terms and prevails on AI-specific data-protection and EU AI Act matters within its scope.

2. DEFINITIONS

“Customer” or “End Customer” means the organisation that controls the tenant: the direct customer, the OEM partner for its own deployment, or the end customer of an Authorized Channel Partner. “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject” and “Personal Data Breach” have the meanings in the GDPR (Regulation (EU) 2016/679); for Swiss data the

Swiss Federal Act on Data Protection (“FADP”) applies with the same meaning. “Sub-processor” means a processor engaged by ORamaVR to process Customer personal data. “Register” means the ORamaVR Sub-Processor Register (OVR-POL-008) at oramavr.com/legal/sub-processors. “Primary Region” means the hosting region stated in Annex 1. Other capitalised terms have the meaning given in the Principal Agreement.

3. THE DATA

3.1 Data subjects. The Customer’s administrators, supervisors, instructors and trainees; Authorized Channel Partner administrators; ORamaVR staff, incidentally.

3.2 Personal data. As listed in Annex 1: account and role data, training sessions and performance data, JARIA voice audio, transcripts, prompts and outputs, support communications and security logs. No real patient data: the Customer must not put patient-identifiable data on the platform or in any JARIA prompt (Exhibit B §4.2(b) and §4.3(a)). If any is found, ORamaVR may delete it and will tell the Customer.

3.3 Purpose. To provide, operate, secure and support the services under the Principal Agreement, on the Customer’s instructions.

3.4 Duration. For the term of the Principal Agreement and the return and deletion period in Section 9.

4. ORAMAVR AS INDEPENDENT CONTROLLER

4.1 Status. For the data described in Section 1.2 as ORamaVR’s own, each party is a separate controller and complies with the data protection law that applies to it. ORamaVR’s processing is described in its Privacy Policy (OVR-POL-002).

4.2 Cooperation. The parties cooperate in good faith on requests from individuals, breaches and authority requests that concern both of them.

5. ORAMAVR AS PROCESSOR

5.1 Status. ORamaVR processes Customer personal data as processor. The Customer is the controller and is responsible for the lawfulness of the processing, including notices to its users.

5.2 Instructions. ORamaVR processes Customer personal data only on the Customer’s documented instructions, including on transfers, unless EU, Member State or Swiss law requires otherwise; in that case ORamaVR informs the Customer beforehand unless the law prohibits it. The Principal Agreement, this DPA, the order and the Customer’s configuration of its tenant are the instructions. ORamaVR immediately informs the Customer if it considers an instruction unlawful. ORamaVR does not sell Customer personal data and does not use it, or any Customer content, to train or fine-tune AI models, unless the Customer opts in under JARIA Terms §5.3.

5.3 Confidentiality. Everyone with access is bound by confidentiality and trained. Access is limited to those who need it.

5.4 Security. ORamaVR applies the security measures in Annex 2 (GDPR Art. 32; FADP Art. 8). It may update them, but not so as to lower the overall level of protection.

5.5 Sub-processors. (a) The Customer authorises the Sub-processors listed in the Register (Annex 3), including ORamaVR’s own affiliates listed there. (b) ORamaVR gives at least 30 days’ notice

before adding or replacing a Sub-processor, by updating the Register and notifying the Customer's contact. (c) The Customer may object on reasonable data-protection grounds within that period, by writing to support@oramavr.com. (d) If an objection is not resolved within 60 days, the Customer may terminate the affected service without penalty. (e) ORamaVR binds each Sub-processor in writing to obligations equivalent to this DPA and remains liable for it.

5.6 Channel partners. Where the Customer came through an Authorized Channel Partner, the Partner may use the Org-Admin Portal only to onboard users, manage the tenant structure, distribute licences and give first-line support. It is bound by equivalent data-protection obligations under its agreement with ORamaVR.

5.7 Requests from individuals. ORamaVR forwards to the Customer, without undue delay, any request it receives from an individual about Customer personal data, and does not answer it unless the Customer asks. It gives the Customer the tools and help reasonably needed to answer requests.

5.8 Assistance. ORamaVR gives the Customer the information and help reasonably needed for its security obligations, breach notifications, data protection impact assessments and prior consultations (GDPR Arts. 32–36). Annex 1, Annex 2 and ORamaVR's AI documentation for JARIA are available for that purpose.

5.9 Breaches. ORamaVR notifies the Customer of a Personal Data Breach affecting Customer personal data without undue delay, and in any event within 72 hours of becoming aware of it. The notice describes, as far as then known, the nature of the breach, the data and number of people affected, the likely consequences and the measures taken or proposed, with a contact point; information may follow in stages. ORamaVR does not notify authorities, individuals or third parties about the Customer's data unless the Customer agrees or the law requires it.

6. JOINT CONTROLLERS

None. If joint control is ever identified, the parties will record their respective responsibilities in writing under GDPR Art. 26.

7. LOCATION AND TRANSFERS

7.1 Primary Region. Customer personal data is hosted in the Primary Region stated in Annex 1. ORamaVR gives 60 days' notice before changing the Primary Region, and Section 5.5(c)–(d) applies to the change.

7.2 Adequate countries. Transfers between the EU/EEA, Switzerland and the United Kingdom rely on their mutual adequacy findings.

7.3 Other countries. Where a Sub-processor processes Customer personal data in a country without adequacy, ORamaVR ensures a valid safeguard: the recipient's certification under the EU–US Data Privacy Framework and its Swiss and UK extensions, or the EU standard contractual clauses (Commission Decision (EU) 2021/914), Module Three where ORamaVR exports as processor, with the Swiss adaptations required by the FDPIC and the UK International Data Transfer Addendum. The Customer authorises ORamaVR to enter into those clauses with the Sub-processor; no separate signature by the Customer is needed. The safeguard for each Sub-processor is stated in the Register.

7.4 Assessments. ORamaVR keeps a transfer impact assessment for each transfer that needs one, reviews it at least yearly, and gives the Customer a summary on request (Annex 4).

8. AUDITS

ORamaVR makes available the information reasonably needed to show compliance with this DPA and allows audits by the Customer or its independent auditor. Audits need 30 days' notice, are limited to once a year except after a Personal Data Breach or a reasonable suspicion of non-compliance, take place in business hours without disrupting operations, and are subject to confidentiality. ORamaVR may answer first with documents and reports; an on-site audit follows only if they do not answer the question. Each party bears its own costs.

9. RETURN AND DELETION

When the Principal Agreement ends, the Customer may export its personal data through the platform, or ask ORamaVR to return it in a common machine-readable format, within 30 days. ORamaVR then deletes Customer personal data from active systems within 90 days of the end of the Principal Agreement; backups are overwritten within 35 days after that. ORamaVR confirms deletion in writing on request. Data the law requires ORamaVR to keep is kept only for that purpose and period.

10. CONTACTS

Data protection: support@oramavr.com. Security incidents: security@oramavr.com. The Customer's contact is the one in the Principal Agreement or order, or as it later notifies.

11. LIABILITY

Each party is liable to individuals as the GDPR and the FADP provide. Between the parties, liability under this DPA is subject to the limitations in the Principal Agreement, except where those limitations cannot apply by law.

12. GOVERNING LAW AND DISPUTES

This DPA is governed by Swiss law, subject to mandatory EU, UK or other data protection law that applies to the processing. For a Customer established in the EU/EEA or the United Kingdom, Section 5 is also governed by the law of the country where the Customer is established, so that it binds ORamaVR under that law (GDPR Art. 28(3)). Disputes follow the dispute-resolution clause of the Principal Agreement. For a public institution, the forum stated in its Institutional Rider (OVR-ADD-JUR-001) applies, and nothing in this DPA waives any immunity the institution has under its own law.

13. GENERAL

13.1 Precedence. Where the standard contractual clauses apply, they prevail for the transfers they govern. Then the JARIA Addendum on AI-specific data-protection and EU AI Act matters; then Annex 5 for United States law matters; then this DPA; then the other Annexes.

13.2 Amendments. ORamaVR may amend this DPA as a Standard-Form Document under the amendment clause of the Principal Agreement, unless the Principal Agreement requires a signed amendment. An amendment may not lower the protection of Customer personal data without the Customer's agreement.

ANNEX 1 — DESCRIPTION OF THE PROCESSING

Item	Details
Controller	The Customer, as identified in the Principal Agreement or order
Processor	ORamaVR SA, 34 route de la Galaise, c/o FONGIT, CH-1228 Plan-les-Ouates, Geneva, Switzerland (CHE-478.871.980) · support@oramavr.com
Data subjects	Section 3.1
Account and role data	Name, e-mail, organisation, role, login and authentication data, licence assignments
Training data	Sessions, scenario steps, scores and performance and competency data, multiplayer session data, reports and exports
JARIA data	Voice audio (processed in real time for speech-to-text and text-to-speech), transcripts, prompts, outputs, serialised scene state and IFU references. Requests to AI providers carry only a technical request ID and the user's words — no name, e-mail address or account ID. A short conversation history is held in memory during the session so that JARIA can follow the dialogue; it is not written to a database and is deleted when the session ends
Creator tenant data	OMEN prompts and generated outputs; authored content
Support and logs	Support tickets and correspondence; access and security logs
Not processed	Real patient data. Special categories of data are not intended (Section 3.2)
Processing	Hosting, storage, computation, AI inference, support, backup, deletion
Frequency	Continuous, for the term of the Principal Agreement
Primary Region	Microsoft Azure West Europe (Amsterdam, Netherlands, EU)
On-premises installations	Where the Customer operates the Platform Components on its own premises, ORamaVR processes Customer personal data in that installation only where the Customer grants it access for support or updates, and then as processor for that access. Artificial-intelligence and speech providers engaged under the Customer's own accounts are the Customer's providers, not Sub-processors
Sub-processors	The Register (Annex 3)

ANNEX 2 — SECURITY MEASURES

- **Encryption.** TLS 1.2 or higher in transit; encryption at rest by the hosting provider's storage encryption.
- **Access.** Role-based, least-privilege access; multi-factor authentication for all staff access to production and administration; named accounts only; access removed promptly when a person leaves or changes role; administrative access logged.
- **Separation.** Logical separation of each Customer tenant.
- **Hosting.** Microsoft Azure data centres, which hold ISO/IEC 27001 and SOC 2 reports issued to Microsoft. ORamaVR itself does not claim a certification.
- **Backups and recovery.** Daily backups kept for no more than 35 days; restoration tested; recovery targets as stated in Exhibit A.
- **Logs.** Security and access logs kept for 90 days, longer only for an active investigation.
- **Development.** Change management for production releases; no production personal data in development or test unless anonymised.

- **Testing.** Regular vulnerability scanning, with findings tracked to remediation; independent penetration testing is planned.
- **Incidents.** Written incident-response procedure with named responders; the 72-hour notice in Section 5.9.
- **People.** Confidentiality obligations and data-protection and security training for all staff and contractors with access.

ANNEX 3 — SUB-PROCESSORS

The authorised Sub-processors, their services, locations and transfer safeguards are listed in the Register at oramavr.com/legal/sub-processors, which has a dated change log. The Register is the only list; it is not restated here. A provider that the Customer engages itself — for example the Customer's own AI account used through its own key ("bring your own key") for OMEN text features — is not an ORamaVR Sub-processor.

ANNEX 4 — TRANSFERS

The safeguard for each transfer is stated in the Register (Section 7.3). Transfer impact assessments are kept for transfers to the United States that rely on standard contractual clauses, and are reviewed at least yearly and whenever the law or the provider's terms change. Supplementary measures include data minimisation (AI requests carry only a technical request ID and the user's words, with no name, e-mail address or account ID), encryption in transit and at rest, and contractual prohibitions on use for model training. Where a provider retains request data for abuse monitoring under its standard terms, the Register says so and states the period.

ANNEX 5 — UNITED STATES TERMS

This Annex applies where the Customer is established in the United States or the processing is subject to US law. It replaces the former US DPA Addendum (OVR-SCH-003-US-EC).

A5.1 FERPA. Where the Customer is subject to FERPA (20 U.S.C. §1232g; 34 C.F.R. Part 99) and discloses education records to ORamaVR, ORamaVR acts as a school official with a legitimate educational interest under the Customer's direct control (34 C.F.R. §99.31(a)(1)). ORamaVR uses education records only to provide the services, does not re-disclose them except as FERPA permits and on the Customer's instructions, and does not use them for advertising or AI training.

A5.2 State privacy laws. Where the California Consumer Privacy Act or a comparable US state privacy law applies, ORamaVR is a service provider or processor. It processes the data only for the business purposes in this DPA and not outside its direct business relationship with the Customer; does not sell or share it; does not combine it with other data except as the law permits; helps the Customer answer consumer requests; allows the Customer to take reasonable steps to check compliance (Section 8) and to stop and remediate unauthorised use; and tells the Customer if it can no longer meet these obligations.

A5.3 Public records. A public-body Customer subject to a public-records law will, where lawful, notify ORamaVR of a request covering ORamaVR's confidential information (including Annex 2 and Sub-processor details) and assert available exemptions before disclosure.

A5.4 US-origin data. Hosting US-origin personal data in the EU is not itself a transfer; onward disclosures follow Section 7.3. ORamaVR binds Sub-processors to obligations no less protective than this Annex for that data.

A5.5 No PHI. ORamaVR does not process protected health information under HIPAA. If a Customer ever needs to supply it, the parties will first sign a business associate agreement for that processing.