Data Processing Agreement (DPA)

Version 2026-04-27

This Data Processing Agreement ("DPA") supplements the main agreement between v9Labs GmbH i.G. ("Processor") and the customer ("Controller") for use of the AI use-case workshop platform and sets out the parties' obligations under Art. 28 GDPR.

1. Subject matter and duration

The processing concerns the provision, security, and billing of the platform. The Processor processes personal data only on documented instructions from the Controller and only to the extent required to perform the main agreement. This DPA applies for the term of the main agreement and for as long as personal data is processed on behalf of the Controller.

2. Nature and purpose of processing

Processing includes manager data for login, payment allocation, and workshop administration; participant email addresses for invitations and authentication; workshop answers to run the AI-assisted interview, create personal participant materials, and create an aggregated report. Optional voice input is transcribed transiently and not stored.

3. Types of personal data

Manager data: name where provided, email address, billing address, VAT ID, payment and order references. Participant data: email address, workshop content as text answers, derived participant materials, technical session data, IP address, and user agent for security and abuse prevention. Special categories of personal data under Art. 9 GDPR are not part of the instructed processing and must not be deliberately entered.

4. Categories of data subjects

Purchasing managers, invited employees or other participants invited by the Controller, and technical contacts of the Controller.

5. Instructions and confidentiality

The Processor processes personal data only on documented instructions from the Controller, including instructions for deletion, export, and restriction of processing. Persons with access to personal data are bound by confidentiality or subject to an appropriate statutory duty of confidentiality.

6. Subprocessors

The Controller grants general authorisation for the subprocessors published at /legal/processors. Changes are announced at least 30 days in advance. The Controller may object for important data-protection reasons. The Processor imposes at least the same level of data-protection obligations on subprocessors and remains responsible for their performance.

7. Technical and organisational measures

TLS 1.3 with HSTS preload on every endpoint.

Server access only via SSH public-key authentication.

Database file with restrictive permissions under the app user.

Daily, AES-encrypted restic backups to a second Hetzner region.

Role-based access restrictions and audit logs.

Strict separation between manager view and participant content: no admin override for individual answers.

8. Assistance to the Controller

The Processor reasonably assists the Controller with data-subject requests, deletion, export, and obligations under Art. 32 to 36 GDPR to the extent the relevant information is available to the Processor. Data-subject requests are forwarded or answered after coordination where they concern the Controller.

9. Third-country transfers

Hosting, AI inference, email delivery, and speech-to-text processing take place in the European Union. There is no US transfer for AI inference; cross-region inference is disabled. Stripe as a subprocessor may process individual operational activities in the US; those transfers are covered by Standard Contractual Clauses and additional safeguards.

10. Personal-data breaches

The Processor informs the Controller without undue delay after becoming aware of a personal-data breach affecting the Controller's data. The notice includes, where available, the nature and scope of the incident, affected data categories, likely consequences, and measures taken or proposed.

11. Deletion and return

Workshop content is deleted automatically 90 days after the participation window ends unless the Controller instructs earlier deletion. Return can be provided as a JSON export while the content is still available. Backups may retain data for up to 30 additional days and are then overwritten in the regular backup cycle.

12. Audit rights

The Controller has the right to verify compliance with the agreed measures. v9Labs provides the necessary information and permits reasonably announced audits during normal business hours, provided the audit does not impair the security, confidentiality, or operational stability of other customers.