

DPA

Version 1.0 | 2026-09-24T06:11:23.602Z

DPA Provider

1. Parties and scope

This Data Processing Agreement (DPA) is made between the company, coach or other business customer identified when registering for or accepting this agreement (the "Controller") and Vebelio, operated by Matthias Stein-Schilling, Hallig-Hooge-Stieg 12, 22846 Norderstedt, Germany (the "Processor").

The Controller's identity, address and authorised representative are recorded in its company profile and the versioned acceptance record. This DPA supplements the applicable main agreement for platform services. For processing on behalf of the Controller, this DPA prevails over conflicting provisions of the main agreement.

2. Subject matter, duration and scope

The Processor provides a digital platform for managing user accounts, access rights, offers, content, communications, memberships, courses, files and other agreed functions. The Processor processes personal data only on documented instructions from the Controller unless Union or Member State law requires processing.

Processing starts when the platform service is activated and ends when it is terminated, subject to the provisions on deletion, return and legally required retention. The subject matter, purpose, data categories, data subjects and processing operations are described in Annex A.

3. Instructions

The Controller is the controller and is solely responsible for the lawfulness of processing and data-subject rights. Documented instructions arise from this DPA, the main agreement, the platform functions and settings selected by the Controller, and additional instructions in text form.

The Processor will promptly inform the Controller if it considers an instruction unlawful. It may suspend execution until the instruction is confirmed, changed or withdrawn where legally required.

4. Processor obligations

The Processor will:

- process data only within documented instructions;
- engage only persons bound by confidentiality or an appropriate statutory duty of confidentiality;
- implement appropriate technical and organisational measures under Article 32 GDPR as described in Annex B;

- assist the Controller, as necessary and reasonable, with data-subject requests, data-protection impact assessments, prior consultations and security incidents;
- notify the Controller without undue delay after becoming aware of a personal-data breach affecting Controller data; and
- be able to demonstrate compliance with this DPA.

5. Controller obligations

The Controller ensures in particular that a legal basis exists, data subjects are informed, required consents are obtained and its content, recipients, access rights and instructions are lawful. It authorises only persons requiring access, keeps credentials confidential and reviews permissions regularly.

The platform is not intended for special categories of personal data under Article 9 GDPR or data relating to criminal convictions under Article 10 GDPR. The Controller processes such data only under a prior express agreement, with a sufficient legal basis and appropriate additional safeguards.

6. Confidentiality and access

The Processor limits access to personal data to persons who require it to perform their tasks. Confidentiality obligations continue after the end of the relevant activity. Support access takes place only where necessary for a specific support, security or maintenance case.

7. Technical and organisational measures

The Processor implements the measures in Annex B to ensure a level of security appropriate to the risk. It may develop those measures further provided that the agreed security level is not materially reduced. On request, the Processor will communicate material security-relevant changes appropriately.

8. Sub-processors

The Controller grants general authorisation for the sub-processors listed in the versioned Annex C. The Processor will enter into an agreement with each sub-processor that preserves at least the data-protection obligations in this DPA.

The Processor will inform the Controller in text form before adding or replacing a sub-processor. The Controller may object within 14 days on important, demonstrable data-protection grounds. If no reasonable alternative is available, the parties may end the affected part of the service under the main agreement.

9. International transfers

Transfers outside the European Union or European Economic Area take place only where Articles 44 et seq. GDPR are met. The Processor uses, in particular, an adequacy decision or appropriate safeguards such as EU Standard Contractual Clauses and required supplementary measures. The relevant basis is recorded in Annex C or disclosed on the Controller's reasoned request.

10. Data-subject rights and assistance

Where a data subject contacts the Processor directly, the Processor will promptly forward the request to the Controller where attribution is possible. It will not answer the request itself unless instructed by the Controller or required by law.

Taking account of the nature of processing and information available to it, the Processor assists the Controller in meeting obligations under Articles 32 to 36 GDPR. Services beyond the contractually owed platform service that were not caused by the Processor may be charged after prior agreement.

11. Personal-data breaches

To the extent available, breach notifications include the nature and time of the incident, affected categories of data and data subjects, approximate numbers, likely consequences, measures taken or proposed, and a contact point. The Processor assists the Controller in assessment and any notification duties.

12. Evidence and audits

On request, the Processor provides information necessary to demonstrate compliance with this DPA. Evidence may include current TOM documentation, self-assessments, audit reports or certifications.

Further audits are permitted with reasonable prior notice, during normal business hours and with respect for security and trade secrets. They must not disproportionately disrupt operations. The Processor may require auditors to sign a confidentiality agreement.

13. Rectification, deletion and return

During the contract, the Processor rectifies, deletes or restricts data on documented instruction where the Controller cannot carry out the action itself through the platform. After the service ends, the Processor deletes or returns all Controller personal data on instruction unless statutory retention duties prevent this.

Backups are not individually altered but overwritten or deleted through regular backup cycles. Data processed by the Processor for its own statutory duties, contract administration, billing, security, abuse prevention or legal defence is not processed as a processor and is unaffected by this provision.

14. Independent responsibility and payment services

The Processor acts as an independent controller where necessary for its own contract with the Controller, invoicing, statutory retention, IT security, abuse prevention, or the establishment, exercise or defence of legal claims.

Payment service providers may be independent controllers depending on the payment integration, especially for payment processing, fraud prevention and regulatory obligations. Their role and the data transmitted are checked and documented in the relevant payment process and in Annex C.

15. Term, amendments and final provisions

This DPA does not end before the main agreement where processing remains necessary to perform it. Amendments require text form and versioned acceptance where they materially affect the contractual processing.

If a provision is or becomes ineffective, the remaining agreement remains effective. Mandatory data-protection law applies; otherwise German law applies.

Annex A - Description of processing

****Subject matter and purpose:**** Provision, operation, security, maintenance and support of the platform for the Controller; management of accounts, roles, access rights, offers, content, communications, courses, memberships, files and, where applicable, customer-related analytics.

****Data subjects:**** The Controller's employees, administrators, coaches, customers, members, subscribers, prospects, participants, communication partners and support contacts.

****Data types:**** Master, contact and address data; account, login, role and permission data; contract, booking and subscription data; communication and content data; uploads; usage, device, IP, security and log data; and, where required for the platform service, payment-status and invoice references.

****Processing operations:**** Collection, recording, organisation, storage, display, making available, transmission on instruction, matching, restriction, deletion, backup, recovery and logging.

Annex B - Technical and organisational measures

- Access control through individual accounts, authentication, HTTPS/TLS, protected administrative areas and role-restricted infrastructure access.

- Access control through tenant-scoped data access, roles, permissions, offer and entitlement checks, and need-to-know access.

- Transfer control through encrypted transmission, authorised storage and database access, contractual sub-processor safeguards and limited support access.

- Input control through attributable user accounts, timestamps, audit trails and security logs for relevant changes.

- Availability and recovery control through backup and recovery procedures, patch management, error monitoring and protection against unauthorised administrative changes.

- Separation through tenant, role and offer boundaries and separate development and production environments where personal data are involved.

- Regular review through permission checks, security and error analysis, and adaptation to new risks or functions.

The concrete technical implementation and operational effectiveness of these measures must be verified against the current production environment before release.

Annex C - Sub-processors and international transfers

Before publication and before any acceptance of this DPA, this annex must be completed and versioned with the sub-processors actually used. Each entry must state at least the organisation, address/country, service, data categories, processing location, role, international-transfer basis and date of prior notice.

Listing planned or inactive services does not authorise their processing. Changes to this annex follow the procedure in section 8.