

AVV Anbieter

1. Parteien und Geltung

Diese Vereinbarung zur Auftragsverarbeitung (AVV) wird zwischen dem bei Registrierung oder Annahme dieser Vereinbarung ausgewiesenen Unternehmen, Coach oder sonstigen Geschäftskunden (nachfolgend „Auftraggeber“) und Vebelio, betrieben von Matthias Stein-Schilling, Hallig-Hooge-Stieg 12, 22846 Norderstedt, Deutschland (nachfolgend „Auftragnehmer“) geschlossen.

Die konkrete Identität, Anschrift und vertretungsberechtigte Person des Auftraggebers ergeben sich aus seinem Unternehmensprofil und dem versionierten Akzeptanznachweis. Diese AVV ergänzt den jeweiligen Hauptvertrag über die Plattformleistungen. Soweit der Auftragnehmer personenbezogene Daten im Auftrag verarbeitet, hat diese AVV Vorrang vor widersprechenden Regelungen des Hauptvertrags.

2. Gegenstand, Dauer und Umfang

Der Auftragnehmer stellt dem Auftraggeber eine digitale Plattform für die Verwaltung von Nutzerkonten, Zugängen, Angeboten, Inhalten, Kommunikation, Mitgliedschaften, Kursen, Dateien und weiteren vereinbarten Funktionen bereit. Dabei verarbeitet er personenbezogene Daten ausschließlich nach dokumentierter Weisung des Auftraggebers, soweit nicht eine Rechtsvorschrift der Union oder eines Mitgliedstaates die Verarbeitung verlangt.

Die Verarbeitung beginnt mit Freischaltung der Plattformleistung und endet mit deren Beendigung, vorbehaltlich der Regelungen zu Löschung, Rückgabe und gesetzlich erforderlicher Aufbewahrung. Gegenstand, Zweck, Datenkategorien, betroffene Personen und Verarbeitungsvorgänge ergeben sich aus Anlage A.

3. Weisungen

Der Auftraggeber ist Verantwortlicher und allein für die Rechtmäßigkeit der Verarbeitung sowie für die Rechte der betroffenen Personen verantwortlich. Dokumentierte Weisungen ergeben sich aus dieser AVV, dem Hauptvertrag, den vom Auftraggeber gewählten Plattformfunktionen und Einstellungen sowie aus zusätzlichen Weisungen in Textform.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er eine Weisung für rechtswidrig hält. Er darf die Ausführung bis zur Bestätigung, Änderung oder Rücknahme der Weisung aussetzen, soweit dies rechtlich erforderlich ist.

4. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich,

- Daten nur im Rahmen der dokumentierten Weisungen zu verarbeiten;

- nur Personen einzusetzen, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
- angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO gemäß Anlage B zu treffen;
- den Auftraggeber bei Betroffenenanfragen, Datenschutz-Folgenabschätzungen, vorherigen Konsultationen und Sicherheitsvorfällen im erforderlichen und zumutbaren Umfang zu unterstützen;
- Datenschutzverletzungen, die Daten des Auftraggebers betreffen, unverzüglich nach Bekanntwerden mitzuteilen;
- die in dieser AVV geregelte Auftragsverarbeitung nachweisen zu können.

5. Pflichten des Auftraggebers

Der Auftraggeber stellt insbesondere sicher, dass eine Rechtsgrundlage besteht, Betroffene informiert werden, notwendige Einwilligungen vorliegen und seine Inhalte, Empfänger, Zugriffsrechte und Weisungen rechtmäßig sind. Er berechtigt nur Personen, die Zugriff benötigen, hält Zugangsdaten vertraulich und überprüft Berechtigungen regelmäßig.

Die Plattform ist nicht für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder Daten über strafrechtliche Verurteilungen nach Art. 10 DSGVO bestimmt. Der Auftraggeber verarbeitet solche Daten nur nach vorheriger ausdrücklicher Vereinbarung und mit einer ausreichenden Rechtsgrundlage sowie geeigneten zusätzlichen Schutzmaßnahmen.

6. Vertraulichkeit und Zugriff

Der Auftragnehmer beschränkt den Zugriff auf personenbezogene Daten auf die Personen, die ihn zur Erfüllung ihrer Aufgaben benötigen. Verpflichtungen zur Vertraulichkeit gelten über das Ende der Tätigkeit hinaus. Supportzugriffe erfolgen nur, soweit sie für einen konkreten Support-, Sicherheits- oder Wartungsfall erforderlich sind.

7. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in Anlage B beschriebenen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus. Er darf diese Maßnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau nicht wesentlich unterschritten wird. Wesentliche sicherheitsrelevante Änderungen teilt er dem Auftraggeber auf Anfrage in geeigneter Form mit.

8. Unterauftragsverarbeiter

Der Auftraggeber erteilt eine allgemeine Genehmigung für die in Anlage C versioniert aufgeführten Unterauftragsverarbeiter. Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter eine Vereinbarung, die mindestens die Datenschutzpflichten dieser AVV wahrt.

Der Auftragnehmer informiert den Auftraggeber vor der Hinzunahme oder Ersetzung eines Unterauftragsverarbeiters in Textform. Der Auftraggeber kann aus wichtigem, nachweisbarem datenschutzrechtlichem Grund binnen 14 Tagen widersprechen. Soweit keine zumutbare Alternative möglich

ist, können die Parteien den betroffenen Teil der Leistung nach den Regelungen des Hauptvertrags beenden.

9. Drittlandübermittlungen

Eine Übermittlung in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Auftragnehmer setzt insbesondere einen Angemessenheitsbeschluss oder geeignete Garantien wie EU-Standardvertragsklauseln und erforderliche ergänzende Maßnahmen ein. Die jeweils relevante Grundlage wird in Anlage C oder auf begründete Anfrage des Auftraggebers ausgewiesen.

10. Betroffenenrechte und Unterstützung

Soweit eine betroffene Person den Auftragnehmer unmittelbar kontaktiert, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung möglich ist. Der Auftragnehmer beantwortet sie nicht selbst, außer der Auftraggeber hat ihn hierzu angewiesen oder eine gesetzliche Pflicht besteht.

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO. Unterstützungsleistungen, die über die vertraglich geschuldete Plattformleistung hinausgehen und nicht vom Auftragnehmer verursacht wurden, können nach vorheriger Abstimmung vergütet werden.

11. Datenschutzverletzungen

Die Meldung einer Datenschutzverletzung enthält, soweit verfügbar, Art und Zeitpunkt des Vorfalls, betroffene Daten- und Personenkategorien, ungefähre Anzahl der Betroffenen und Datensätze, wahrscheinliche Folgen, bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen sowie einen Ansprechpartner. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Bewertung und etwaigen Melde- oder Benachrichtigungspflichten.

12. Nachweise und Kontrollen

Der Auftragnehmer stellt auf Anfrage die Informationen zur Verfügung, die für den Nachweis der Einhaltung dieser AVV erforderlich sind. Der Nachweis kann durch aktuelle TOM-Dokumentation, Selbstauskünfte, Prüfberichte oder Zertifikate erfolgen.

Weitergehende Prüfungen sind nach angemessener Vorankündigung, während üblicher Geschäftszeiten und unter Wahrung von Sicherheits- und Geschäftsgeheimnissen zulässig. Sie dürfen den Betrieb nicht unverhältnismäßig beeinträchtigen. Der Auftragnehmer kann eine Vertraulichkeitsvereinbarung für Prüfer verlangen.

13. Berichtigung, Löschung und Rückgabe

Während der Vertragslaufzeit berichtigt, löscht oder beschränkt der Auftragnehmer Daten nach dokumentierter Weisung, soweit der Auftraggeber dies nicht selbst über die Plattform ausführen kann. Nach Ende der Leistung löscht oder gibt der Auftragnehmer auf Weisung alle personenbezogenen Daten des Auftraggebers zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

Backups werden nicht isoliert verändert, sondern im Rahmen der regulären Backup-Zyklen überschrieben oder gelöscht. Daten, die der Auftragnehmer für eigene gesetzliche Pflichten, Vertragsverwaltung, Abrechnung, Sicherheit, Missbrauchsprävention oder Rechtsverteidigung verarbeitet, werden nicht als Auftragsverarbeiter verarbeitet und bleiben von dieser Regelung unberührt.

14. Eigene Verantwortlichkeit und Zahlungsdienste

Der Auftragnehmer verarbeitet Daten in eigener Verantwortlichkeit, soweit dies für den eigenen Vertrag mit dem Auftraggeber, Rechnungsstellung, gesetzliche Aufbewahrung, IT-Sicherheit, Missbrauchsprävention oder die Durchsetzung und Abwehr von Ansprüchen erforderlich ist.

Zahlungsdienstleister können je nach konkreter Zahlungsintegration eigenständig Verantwortliche sein, insbesondere für Zahlungsabwicklung, Betrugsprävention und regulatorische Pflichten. Ihre Rolle und die übermittelten Daten werden im jeweiligen Zahlungsprozess und in Anlage C geprüft und dokumentiert.

15. Laufzeit, Änderungen und Schlussbestimmungen

Diese AVV endet nicht vor dem Hauptvertrag, soweit die Auftragsverarbeitung für dessen Durchführung erforderlich ist. Änderungen dieser AVV bedürfen der Textform und einer versionierten Annahme, soweit sie die vertragliche Auftragsverarbeitung wesentlich betreffen.

Sollte eine Regelung unwirksam sein oder werden, bleibt der übrige Vertrag wirksam. Es gelten die zwingenden datenschutzrechtlichen Vorschriften; im Übrigen gilt deutsches Recht.

Anlage A - Beschreibung der Verarbeitung

****Gegenstand und Zweck:**** Bereitstellung, Betrieb, Absicherung, Wartung und Support der Plattform für den Auftraggeber; Verwaltung von Konten, Rollen, Zugängen, Angeboten, Inhalten, Kommunikation, Kursen, Mitgliedschaften, Dateien und gegebenenfalls kundenbezogenen Auswertungen.

****Betroffene Personen:**** Mitarbeiter, Administratoren, Coaches, Kunden, Mitglieder, Abonnenten, Interessenten, Teilnehmer, Kommunikationspartner und Supportkontakte des Auftraggebers.

****Datenarten:**** Stammdaten, Kontakt- und Adressdaten, Konto-, Login-, Rollen- und Berechtigungsdaten, Vertrags-, Buchungs- und Abonnementdaten, Kommunikations- und Inhaltsdaten, Uploads, Nutzungs-, Geräte-, IP-, Sicherheits- und Protokolldaten sowie soweit für die Plattformleistung erforderlich Zahlungsstatus- und Rechnungsreferenzen.

****Verarbeitungsvorgänge:**** Erheben, Erfassen, Organisieren, Speichern, Anzeigen, Bereitstellen, Übermitteln auf Weisung, Abgleichen, Einschränken, Löschen, Sichern, Wiederherstellen und Protokollieren.

Anlage B - Technische und organisatorische Maßnahmen

- Zugangskontrolle durch individuelle Konten, Authentifizierung, HTTPS/TLS, Schutz administrativer Bereiche und rollenbeschränkten Infrastrukturzugriff.

- Zugriffskontrolle durch mandantenbezogene Datenzugriffe, Rollen, Rechte, Angebots- und Zugangsprüfungen sowie das Need-to-know-Prinzip.

- Weitergabekontrolle durch verschlüsselte Übertragung, autorisierte Storage- und Datenbankzugriffe, vertragliche Bindung von Unterauftragsverarbeitern und begrenzte Supportzugriffe.
- Eingabekontrolle durch zuordenbare Benutzerkonten, Zeitstempel, Audit- und Sicherheitsprotokolle für relevante Änderungen.
- Verfügbarkeits- und Wiederherstellungskontrolle durch Backup- und Wiederherstellungsverfahren, Patchmanagement, Fehlerbeobachtung und Schutz vor unberechtigten administrativen Eingriffen.
- Trennung durch Mandanten-, Rollen- und Angebotsgrenzen sowie getrennte Entwicklungs- und Produktivumgebungen, soweit personenbezogene Daten betroffen sind.
- Regelmäßige Überprüfung durch Rechteprüfung, Sicherheits- und Fehleranalyse sowie Anpassung bei neuen Risiken oder Funktionen.

Die konkrete technische Umsetzung und die Betriebswirksamkeit der Maßnahmen sind vor Freigabe anhand der aktuellen Produktionsumgebung zu prüfen.

Anlage C - Unterauftragsverarbeiter und Drittlandtransfers

Diese Anlage muss vor Veröffentlichung und vor jeder Annahme als AVV mit den tatsächlich eingesetzten Unterauftragsverarbeitern vervollständigt und versioniert werden. Je Eintrag sind mindestens Unternehmen, Anschrift/Land, Leistung, Datenkategorien, Verarbeitungsort, Rolle, Rechtsgrundlage einer Drittlandübermittlung und Datum der Vorabinformation aufzunehmen.

Eine Nennung geplanter oder inaktiver Dienste ist keine Freigabe ihrer Verarbeitung. Änderungen dieser Anlage folgen dem Verfahren aus Abschnitt 8.