

Vereinbarung zur Auftragsverarbeitung für Plexbook

nach Art. 28 DSGVO | Stand: 19.10.2026 | Version 1.0

Parteien

Der Kunde gemäß den AGB für Plexbook, im Folgenden **Verantwortlicher**

und

Proplex GmbH, Seestraße 21, 9500 Villach, Österreich, FN 657479g, UID ATU82353579, im Folgenden **Auftragsverarbeiter**

Abschluss

Diese Vereinbarung ist Anlage zu den AGB für Plexbook. Sie wird mit der Registrierung und der Annahme der AGB abgeschlossen und gilt ohne gesonderte Unterschrift. Der Verantwortliche kann sie jederzeit unter [plexbook.io/avv](https://www.plexbook.io/avv) abrufen und speichern.

1. Gegenstand und Dauer

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die Software Plexbook (Buchung, Bezahlung und Verwaltung von Kursen, Trainings und Dienstleistungen) als Software-as-a-Service bereit. Dabei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen.

(2) Diese Vereinbarung gilt für die Dauer des Vertrags über Plexbook und darüber hinaus, solange der Auftragsverarbeiter Daten des Verantwortlichen verarbeitet (Abschnitt 9).

2. Art und Zweck der Verarbeitung

Die Verarbeitung umfasst Speichern, Ordnen, Auslesen, Verwenden, Übermitteln, Einschränken und Löschen personenbezogener Daten, soweit dies für die Bereitstellung von Plexbook erforderlich ist, insbesondere:

- Verwaltung von Angeboten, Terminen, Buchungen, Wartelisten, Abos, Blockkarten und Gutscheinen
- Verwaltung von Teilnehmer:innen und Anwesenheiten
- Erstellung und Versand von Rechnungen, Gutschriften und Bestätigungsmails
- Verwaltung von Team-Mitgliedern, Einsatzplanung und Honorarabrechnung
- Versand von E-Mails, die der Verantwortliche über Plexbook auslöst
- Betrieb, Sicherung, Wiederherstellung und Fehlerbehebung

Eine Verarbeitung dieser Daten zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

Abgrenzung: Das Login-Konto der Teilnehmer:innen (Name, E-Mail-Adresse, Zugangsdaten) gehört zu Plexbook; dafür ist der Auftragsverarbeiter selbst verantwortlich, weil es bei mehreren Kunden genutzt werden kann. Sobald jemand beim Verantwortlichen bucht, sind die dafür nötigen Daten aber auch Daten des Verantwortlichen, und für sie gilt diese Vereinbarung.

3. Art der Daten und Kreis der Betroffenen

Betroffene: Teilnehmer:innen und Interessent:innen des Verantwortlichen, Personen, für die gebucht wird (auch Kinder), Erziehungsberechtigte, Team-Mitglieder des Verantwortlichen (Admins, Trainer:innen).

Datenarten:

- Stammdaten und Kontaktdaten der Kundschaft (Name, E-Mail-Adresse, Telefonnummer, Anschrift)
- Daten zu Teilnehmer:innen (Name, E-Mail-Adresse, Geburtsdatum, Erfahrungsstufe), häufig von Kindern
- Buchungs-, Vertrags-, Wartelisten- und Anwesenheitsdaten
- Zahlungs- und Rechnungsdaten (Beträge, Zahlungsstatus, Stripe-Kennungen, letzte 4 Ziffern der Karte; **keine** vollständigen Kartendaten, diese verarbeitet ausschließlich Stripe)
- Angaben aus Formularen, die der Verantwortliche selbst anlegt, samt IP-Adresse und Browser-Kennung zur Missbrauchsabwehr (gelöscht nach 7 Tagen)
- Daten von Team-Mitgliedern (Name, Kontaktdaten, Einsätze, Honorare, freiwilliges Profilbild)
- Kommunikationsdaten (Empfänger, Betreff, Zustellstatus von E-Mails, gelöscht nach 90 Tagen)
- Push-Kennungen von Geräten, wenn Mitteilungen eingeschaltet werden
- Protokolldaten (z. B. Änderungen von Rechten mit Zeitpunkt)

Besondere Kategorien nach Art. 9 DSGVO (z. B. Gesundheitsangaben in Formularen) werden nur verarbeitet, soweit der Verantwortliche sie selbst erhebt. Er trägt dafür die Verantwortung.

4. Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Weisungen erteilt der Verantwortliche durch die Nutzung und Konfiguration von Plexbook sowie in Textform an support@plexbook.io.

(2) Weisungsberechtigt sind die Admins des Verantwortlichen in Plexbook.

(3) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit und darf die Ausführung bis zur Bestätigung aussetzen.

5. Vertraulichkeit

Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt über das Ende ihrer Tätigkeit hinaus.

6. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 1** beschriebenen Maßnahmen nach Art. 32 DSGVO.

(2) Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

7. Unterauftragsverarbeiter

- (1) Der Verantwortliche stimmt dem Einsatz der in **Anlage 2** genannten Unterauftragsverarbeiter zu.
- (2) Neue oder geänderte Unterauftragsverarbeiter kündigt der Auftragsverarbeiter mindestens **14 Tage** vorher per E-Mail an und veröffentlicht die aktuelle Liste unter plexbook.io/avv. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kann keine Lösung gefunden werden, kann er den Vertrag über Plexbook mit Wirkung zum Einsatz des neuen Unterauftragsverarbeiters kündigen.
- (3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieser Vereinbarung entsprechen.
- (4) Übermittlungen in Drittländer erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (z. B. EU-US Data Privacy Framework) oder von Standardvertragsklauseln der EU-Kommission.

8. Unterstützung des Verantwortlichen

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen im erforderlichen Umfang bei
 - der Beantwortung von Anfragen betroffener Personen (Art. 12 bis 23 DSGVO), soweit der Verantwortliche diese nicht mit den Funktionen von Plexbook selbst erledigen kann,
 - der Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO),
 - Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 35, 36 DSGVO).
- (2) Der Auftragsverarbeiter informiert den Verantwortlichen **unverzüglich, möglichst binnen 48 Stunden**, nachdem ihm eine Verletzung des Schutzes der Daten des Verantwortlichen bekannt geworden ist, und übermittelt die Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie ihm vorliegen.
- (3) Anfragen Betroffener, die beim Auftragsverarbeiter eingehen und Daten des Verantwortlichen betreffen, leitet er unverzüglich an den Verantwortlichen weiter.

9. Löschung und Rückgabe

- (1) Endet der Vertrag über Plexbook, wird die Organisation des Verantwortlichen inaktiv gestellt. Bis zur Löschung kann der Verantwortliche seine Daten im Dashboard als ZIP-Datei herunterladen (§ 16 der [AGB](#)).
- (2) **30 Tage nach der Inaktivierung** löscht der Auftragsverarbeiter alle Daten des Verantwortlichen, einschließlich Rechnungen, Belegen und Dateien, nach Ankündigung 14, 7 und 1 Tag vorher. Sicherungskopien werden im regulären Zyklus überschrieben, spätestens 30 Tage nach der Löschung.
- (3) Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters bleiben unberührt.

10. Nachweise und Überprüfungen

- (1) Der Auftragsverarbeiter weist die Einhaltung dieser Vereinbarung auf Anfrage nach, in der Regel durch Auskunft, Dokumentation und Berichte seiner Unterauftragsverarbeiter.
- (2) Überprüfungen, auch durch einen vom Verantwortlichen beauftragten, zur Verschwiegenheit verpflichteten Prüfer, erfolgen vorrangig anhand von Unterlagen. Überprüfungen vor Ort sind nach Ankündigung mit angemessener Frist von mindestens 30 Tagen, höchstens einmal pro Kalenderjahr, während der Geschäftszeiten und ohne Störung des Betriebs zulässig. Die Kosten trägt der Verantwortliche, außer die Prüfung ergibt einen erheblichen Verstoß.

11. Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO.

(2) Bei Widersprüchen geht diese Vereinbarung den AGB vor, soweit es um den Schutz personenbezogener Daten geht.

(3) Es gilt österreichisches Recht. Gerichtsstand ist das für 9500 Villach sachlich zuständige Gericht, soweit gesetzlich zulässig.

Anlage 1: Technische und organisatorische Maßnahmen

Bereich	Maßnahme
Zutritt	Verarbeitung ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland (Falkenstein, Nürnberg) mit deren Zutrittskonzepten. Keine Speicherung von Kundendaten in Büroräumen.
Zugang	Persönliche Benutzerkonten, Server-Zugriff ausschließlich per SSH-Schlüssel (Passwort-Login abgeschaltet), keine geteilten Passwörter. Passwörter der Nutzer:innen nur als Hash gespeichert.
Zugriff	Rollen- und Rechtesystem in Plexbook (Admin, Trainer:in) mit Protokoll jeder Rechteänderung. Prüfung der Berechtigung in allen schreibenden Schnittstellen. Produktivzugriff nur für den betreuenden Personenkreis von Proplex. Getrennte Entwicklungs- und Produktivumgebung.
Trennung	Mandantentrennung auf Datenbankebene: Row Level Security auf allen Tabellen. Profilbilder und Belege in privaten Speicherbereichen, nur über kurzlebige signierte Links abrufbar.
Weitergabe	Transportverschlüsselung (TLS) für alle Verbindungen. Keine Weitergabe an Dritte außerhalb Anlage 2.
Eingabe	Protokollierung von Rechteänderungen und von E-Mail-Versand (Empfänger, Betreff, Zustellstatus).
Verfügbarkeit	Tägliche automatische Sicherung der Datenbank. Gespeicherte Dateien liegen im Hetzner Object Storage mit Versionierung und werden zusätzlich in einen zweiten Speicherort in Deutschland kopiert. Aufbewahrung der Sicherungen 30 Tage. Wiederherstellung erprobt (Umzug am 12.10.2026).
Belastbarkeit	Überwachung der Dienste, automatischer Neustart bei Ausfall, Fehlerberichte über Sentry, Benachrichtigung bei Störungen.
Datensparsamkeit	Kartendaten verarbeitet ausschließlich Stripe. IP-Adressen aus Formularen werden nach 7 Tagen gelöscht, E-Mail-Protokolle nach 90 Tagen. Fehlerberichte an Sentry ohne IP-Adresse, Cookies, Namen oder E-Mail-Adressen. Spamschutz für Demo und Kontaktformular selbst betrieben (ALTCHA), ohne Drittanbieter.
Überprüfung	Regelmäßige Aktualisierung der eingesetzten Software, automatisierte Tests der Zugriffsregeln, Sicherheitsaudit vor dem Go-live (05.10.2026), Überprüfung dieser Maßnahmen bei wesentlichen Änderungen.

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage für Drittland
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server, Datenbank, Dateispeicher und Sicherungen	Deutschland (Falkenstein, Nürnberg)	-
Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA	Versand von E-Mails (Bestätigungen, Rechnungen, Login-Mails)	Versand über Irland, Verarbeitung auch in den USA	EU-US Data Privacy Framework und Standardvertragsklauseln
Functional Software, Inc. (Sentry), 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Fehlerberichte aus Dashboard und Shop, ohne IP-Adresse und ohne Namen oder E-Mail- Adressen	EU-Datenregion von Sentry	EU-US Data Privacy Framework
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Schutz vor automatisierten Anfragen (Turnstile), nur wenn sich Gäste ohne Konto im Shop auf eine Warteliste setzen	weltweites Netz, auch USA	EU-US Data Privacy Framework

Keine Unterauftragsverarbeiter von Proplex:

- **Stripe** verarbeitet Zahlungen der Teilnehmer:innen auf Grundlage des eigenen Vertrags zwischen dem Verantwortlichen und Stripe.
- **Google** und **Apple** erhalten Daten nur, wenn sich Personen selbst für die Anmeldung mit diesen Konten entscheiden.
- **Push-Dienste der Browser-Hersteller** (z. B. Google, Mozilla, Apple, Microsoft) stellen Mitteilungen nur zu, wenn eine Person sie selbst einschaltet. Der Inhalt ist Ende-zu-Ende verschlüsselt und enthält keine Namen oder Beträge.