Auftragsverarbeitungsvertrag (AVV)

Fassung vom 1. November 2026

Parteien: Kunde („Verantwortlicher") und der Anbieter („Auftragnehmer"). Zustandekommen: automatisch mit Vertragsschluss (§ 11 Abs. 4 AGB), elektronische Form (Art. 28 Abs. 9 DSGVO). Ansprechpartner für Datenschutz beim Auftragnehmer: Jürgen Thiemann, datenschutz@pulsenorth.ai.

1. Gegenstand / Dauer / Art / Zweck

Der Auftragnehmer verarbeitet personenbezogene Daten nur, um die Funktionen der Plattform bereitzustellen, die der Verantwortliche nutzt. Dauer: Laufzeit des Hauptvertrags (Aufbewahrung und Löschung siehe Ziffer 7). Je Funktion:

– Konto, Anmeldung und Rollen (alle Anwendungen): Firmen-Admins, Mitglieder und Lernende; Name, E-Mail-Adresse, Firma, Rolle, Gruppen, Anmeldezeitpunkte; für Zugang, Rechte und die Zuordnung zum Unternehmen.

– Kurserstellung (Learning Studio): Autorinnen und Autoren sowie Personen, die in hochgeladenem Material vorkommen (soll vermieden werden); Briefings, hochgeladene Dokumente, erzeugte Kurstexte, Prüffragen, Skripte, Sprecherbild und Stimme; für den KI-gestützten Entwurf von Kursen, Übersetzungen und Kursvideos.

– Kurs-Auslieferung und Nachweise (Learning Studio, Hub): vom Verantwortlichen eingeladene Lernende; Name, E-Mail-Adresse, Lernfortschritt, Antworten, Ergebnis, Bearbeitungszeit, Zertifikat, Vorsätze und Transfer-Aufgaben, Beiträge im Kurs; für die Bereitstellung der Kurse, Teilnahme-Nachweise und Erinnerungen. Lernergebnisse werden nicht durch KI-Modelle verarbeitet und nicht zu Trainingszwecken genutzt.

– Gesprächsübungen (Coach): Mitglieder; Gesprächstext mit der KI, auf Wunsch Spracheingabe (Diktat oder Live-Gespräch; freiwillig, vor der ersten Nutzung mit Hinweis; wird verarbeitet, aber nicht als Aufnahme gespeichert), Auswertung mit Punktwerten und Zitaten; für die Übung und die Rückmeldung an die übende Person. Das Ergebnis sieht nur sie selbst.

– Kompetenz-Radar (Hub): Mitglieder; Kompetenzwerte aus den Gesprächsübungen mit Belegzitaten, Selbsteinschätzung, Soll-Profil; für die persönliche Entwicklungsübersicht. Werte für Teams erscheinen nur als Durchschnitt ab fünf Personen, ohne Ranglisten.

– Wissensinterviews (Jobmap): interviewte Beschäftigte sowie im Interview genannte Dritte (soll vermieden werden); Interviewtexte, Zusammenfassungen, Wissenskarten, Stellenprofile; für die KI-gestützte Sicherung von Erfahrungswissen und Übergaben. Die interviewte Person erhält vor dem Interview einen Hinweis; das Unternehmen kann zusätzlich ihre Einwilligung verlangen.

– Assistent (Hilfe-Chat und Kurs-Assistent): Nutzende; Fragen und Antworten, beim Kurs-Assistenten der aktuelle Kursabschnitt; für die Beantwortung von Fragen zur Plattform und

zum Kurs.

– Lernwünsche und Rückmeldungen: Mitglieder und Lernende; Wunsch- und Beitragstexte, Name, Stimmen und Reaktionen; für Bedarfsermittlung und Kursverbesserung.

– Hinweise und Einwilligungen (alle Anwendungen): Nutzende; welche Fassung eines Hinweises sie bestätigt und welche Einwilligung sie erteilt oder widerrufen haben; als Nachweis für den Verantwortlichen.

– Betrieb und Sicherheit: alle Nutzenden; technische Protokolle ohne Ergebnisse und Bewertungen, Fehlerberichte; für Fehlerbehebung und Missbrauchsabwehr.

Für KI-gestützte Funktionen werden nur die jeweils nötigen Inhalte an die in Anlage 2 genannten KI-Dienste übermittelt. Der Auftragnehmer nutzt die Daten nicht zum Training von KI-Modellen; was die einzelnen Dienste speichern und nutzen dürfen, steht in Anlage 2.

2. Weisungsbindung

Verarbeitung nur auf dokumentierte Weisung; die funktionsgemäße Nutzung des Dienstes gilt als Weisung.

Weisungen erteilt der Verantwortliche auch über die Einstellungen in der Verwaltung, zum Beispiel zu KI-Funktionen, Hinweisen und Einwilligungen oder zur Aufbewahrung (Ziffer 7). Jede Änderung wird protokolliert.

Hält der Auftragnehmer eine Weisung für einen Verstoß gegen Datenschutzrecht, teilt er das dem Verantwortlichen unverzüglich mit.

Der Auftragnehmer nutzt die Daten ausschließlich, um die Leistungen für den Verantwortlichen zu erbringen. Er verkauft sie nicht und verwendet sie weder für Werbung noch für eigene Zwecke.

3. Vertraulichkeit und Zugriffe des Auftragnehmers

Verpflichtung der eingesetzten Personen auf Vertraulichkeit.

Beschäftigte des Auftragnehmers greifen auf Daten des Verantwortlichen nur zu, um Störungen zu beheben, oder auf Weisung des Verantwortlichen. Jeder solche Zugriff wird manipulationssicher protokolliert, mit Zeitpunkt, Person, Unternehmen und Aktion. Das Protokoll lässt sich nur ergänzen, nicht ändern oder löschen.

4. Sicherheit (Art. 32)

Technische und organisatorische Maßnahmen gemäß Anlage 1 (TOM).

5. Subunternehmer

Der Verantwortliche genehmigt die in Anlage 2 und unter pulsenorth.ai/unterauftragsverarbeiter genannten Subunternehmer.

Neue oder ersetzte Subunternehmer kündigt der Auftragnehmer mindestens 30 Tage vor ihrem Einsatz an: per E-Mail an die Admins des Verantwortlichen und im Änderungsverlauf der Dienstleister-Seite.

Der Verantwortliche kann binnen 30 Tagen nach der Ankündigung mit Begründung widersprechen. Der Auftragnehmer bietet dann eine Lösung ohne den neuen Subunternehmer an, zum Beispiel indem er die betroffene Funktion für den Verantwortlichen abschaltet. Gelingt das nicht binnen 30 Tagen, kann der Verantwortliche die betroffenen Leistungen ohne Vertragsstrafe kündigen; bereits bezahlte, ungenutzte Credits erstattet der Auftragnehmer.

6. Unterstützung

Unterstützung bei Betroffenenrechten und bei Art. 32–36 DSGVO im Rahmen des technisch Möglichen.

Wendet sich eine betroffene Person direkt an den Auftragnehmer, zum Beispiel mit einem Auskunfts- oder Löschwunsch, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter.

7. Aufbewahrung, Löschung und Rückgabe

Wie lange Daten während der Vertragslaufzeit aufbewahrt werden, legt der Verantwortliche als dauerhafte Weisung fest: Seine Admins wählen die Fristen in der Verwaltung unter Einstellungen › Datenschutz; jede Änderung wird protokolliert. Wählen sie nichts, gilt der Standard.

– Lernstands- und Nachweisdaten gehosteter Kurse werden gelöscht, wenn seit dem letzten Kurszugriff 24 Monate (Standard), 36, 60 oder 120 Monate vergangen sind.

– Konten deaktivierter Personen, zum Beispiel ausgeschiedener Beschäftigter, werden 12 Monate (Standard), 24, 36 oder 60 Monate nach der Deaktivierung anonymisiert: Name und E-Mail-Adresse werden entfernt, Nachweise bleiben ohne Namen erhalten. 30 Tage vor jeder Anonymisierung erhalten alle Admins des Verantwortlichen eine E-Mail, damit sie Nachweise vorher exportieren können.

Der Verantwortliche kann Daten jederzeit früher löschen. Exportierte Nachweise (CSV/PDF) verbleiben beim Verantwortlichen; braucht er Nachweise länger, als die gewählte Frist reicht, obliegt ihm die Archivierung.

Nach Vertragsende hat der Verantwortliche 30 Tage Zugang, um seine Daten zu exportieren. Danach löscht der Auftragnehmer die Daten, soweit keine gesetzliche Aufbewahrung (z. B. Rechnungsdaten, § 147 AO) entgegensteht; Sicherungen laufen binnen weiterer 7 Tage aus. Auf Wunsch bestätigt der Auftragnehmer die Löschung schriftlich.

8. Nachweis / Audit

Bereitstellung erforderlicher Informationen; Audits über Zertifikate/Berichte, ergänzend Vor-Ort-Prüfung nach Ankündigung.

9. Drittland

Übermittlungen nur mit Garantien nach Kap. V DSGVO (SCC/Angemessenheit) – siehe Anlage 2.

10. Datenpannen

Der Auftragnehmer informiert den Verantwortlichen unverzüglich, möglichst innerhalb von 24 Stunden, nachdem er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat.

Die Meldung enthält, soweit bekannt: was passiert ist; welche Arten und ungefähr wie viele Personen und Datensätze betroffen sind; einen Ansprechpartner für Rückfragen; die wahrscheinlichen Folgen; die ergriffenen oder geplanten Maßnahmen, auch um nachteilige Folgen zu mildern. Was noch nicht bekannt ist, reicht der Auftragnehmer nach, sobald er es weiß.

Der Auftragnehmer unterstützt den Verantwortlichen bei der Aufklärung der Ursache und bei dessen Meldungen an Aufsichtsbehörde und Betroffene (Art. 33 und 34 DSGVO) und beseitigt die Ursache, soweit sie in seinem Bereich liegt.

11. Anfragen von Behörden und Dritten

Verlangt eine Behörde oder ein Dritter Daten des Verantwortlichen heraus, informiert der Auftragnehmer den Verantwortlichen unverzüglich, soweit das Gesetz es nicht verbietet. Er gibt die Daten nur mit Zustimmung des Verantwortlichen heraus, es sei denn, er ist gesetzlich dazu verpflichtet.

Anlage 1 — Technische und organisatorische Maßnahmen (TOM)

– Verschlüsselung in Transport und Speicherung; Webhook kryptografisch abgesichert.

– Zugriffskontrolle über Authentifizierung und Workspace-/Team-Berechtigung; keine öffentlichen URLs.

– Kurzlebige Zugriffstoken: SAS-Download-Links mit 2 Minuten Lebensdauer.

– Identitätsmanagement: Managed Identities statt rotierender Passwörter/Zugangsschlüssel.

– Zugriffe von Beschäftigten des Auftragnehmers nur zur Störungsbehebung oder auf Weisung; jeder Zugriff wird in einem nur ergänzbaren, unveränderlichen Protokoll festgehalten (Zeitpunkt, Person, Unternehmen, Aktion).

– Datenminimierung: Trennung von Rechnungs- und Analyse-/Transkriptdaten; Rechnungslayout nur mit Pflichtangaben.

– Integrität/GoBD: unveränderbare, lückenlos nummerierte Rechnungsablage; atomare Datenbank-Transaktionen.

– Datenminimierte Verarbeitung der Eingaben; keine Trainingsnutzung durch den Auftragnehmer. Bei Google Cloud Vertex AI ist der Zwischenspeicher seit dem 1. November 2026 abgeschaltet; zur Abwehr von Missbrauch kann Google von seinen Filtern markierte Anfragen bis zu 90 Tage aufbewahren und von befugten Mitarbeitenden prüfen lassen. Gespeicherte Inhalte (Kurse, Rollenspiele, Interviews, Lernstände) unterliegen den Fristen in Ziffer 7.

– Kurs-Auslieferung: personengebundene, kryptografisch signierte, zeitlich befristete und jederzeit widerrufbare Einladungs-Links; keine Konten und keine Passwörter für Lernende (Datenminimierung); Ausschluss von Suchmaschinen-Indexierung; Zugriffsbegrenzung (Rate-Limiting).

Anlage 2 — Subunternehmer

Microsoft Azure (Compute, Cosmos DB, Blob Storage) – Hosting, Daten-/Rechnungsspeicherung – Region EU (Westeuropa, Niederlande) – EU-intern.

Google Cloud Vertex AI einschließlich gehosteter Partnermodelle (Gemini, Claude) in der EU (Google Cloud EMEA Ltd., Irland) – Text-KI aller Anwendungen: Kurserstellung und Video-Regie (Studio), Gesprächsübung einschließlich Live-Gespräch (Coach), Wissensinterviews (Jobmap), Assistent – Region EU (Mehrfachregion EU; Einbettungen für die Suche in Frankfurt) – EU-intern; keine Nutzung zum Training; Zwischenspeicher seit dem 1. November 2026 abgeschaltet; zur Abwehr von Missbrauch kann Google von seinen Filtern markierte Anfragen bis zu 90 Tage aufbewahren und von befugten Mitarbeitenden prüfen lassen.

Microsoft (Azure AI Speech) – Spracherkennung (Diktat im Coach) und Sprachausgabe (Studio) – Region EU (Westeuropa) – EU-intern; keine Speicherung der Aufnahmen.

DeepL SE (Köln) – Übersetzung von Kurstexten, keine Daten von Lernenden – weltweit: seit dem 1. Januar 2026 in AWS-Regionen in der EU, den USA und Japan – EU-Standardvertragsklauseln (Art. 46 DSGVO); Texte werden nur vorübergehend für die Übersetzung verarbeitet, Glossare bleiben bis zur Löschung gespeichert; nur der bezahlte Plan.

fal.ai (Features and Labels Inc., USA) – Bilder und Avatar-Videos für Kursvideos im Learning Studio aus Skripttext und synthetischen Sprecherbildern; standardmäßig keine personenbezogenen Daten – USA – EU-Standardvertragsklauseln (Art. 46 DSGVO); Ein- und Ausgaben werden bei fal.ai nicht gespeichert (bei jedem Auftrag abgeschaltet), erzeugte Dateien verfallen dort nach einer Stunde, die Ergebnisse gehen sofort in den eigenen Speicher des Auftragnehmers.

Microsoft 365 (Exchange Online) – Versand von System-E-Mails – Region EU – EU-intern.

Nicht in dieser Liste: Stripe wickelt Zahlungen als eigenständig Verantwortlicher ab, nicht im Auftrag (siehe Datenschutzerklärung).