Auftragsverarbeitungsvertrag (AVV)

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") regelt die datenschutzrechtlichen Rechte und Pflichten zwischen dem Kunden als Verantwortlichem und der SpecialEffX UG (haftungsbeschränkt), Franz-von-Füll-Straße 8, 86922 Eresing, Deutschland, als Auftragsverarbeiter im Zusammenhang mit der Erbringung der im Hauptvertrag definierten Leistungen. Der AVV konkretisiert die Anforderungen des Art. 28 der Datenschutz-Grundverordnung (DSGVO). Bei Widersprüchen zwischen den Bestimmungen dieses AVV und denen des Hauptvertrages gehen die Regelungen dieses AVV vor, soweit es sich um Fragen des Schutzes personenbezogener Daten im Rahmen der Auftragsverarbeitung handelt.

§ 1 Gegenstand, Dauer und Spezifikation der Verarbeitung

1.1 Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen, die sich aus der Erbringung des SaaS-Dienstes „MeetEffX" gemäß dem zwischen den Parteien geschlossenen Hauptvertrag (nachfolgend „Hauptvertrag") ergibt.

1.2 Die Dauer dieses AVV richtet sich nach der Laufzeit des Hauptvertrages. Als Hauptvertrag gilt auch ein unentgeltlicher Nutzungsvertrag, insbesondere während und nach einer Testphase ohne hinterlegtes Zahlungsmittel. Dieser AVV beginnt mit der ersten Nutzung des Dienstes, unabhängig davon, ob für die Nutzung ein Entgelt geschuldet ist.

1.3 Die Spezifikation der Verarbeitung, insbesondere Art und Zweck der Verarbeitung, die Art der zu verarbeitenden personenbezogenen Daten und der Kreis der betroffenen Personen, sind in Anlage 1 zu diesem Vertrag abschließend festgelegt.

§ 2 Weisungsrecht des Verantwortlichen

2.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der Vereinbarungen dieses AVV und nach dokumentierten Weisungen des Verantwortlichen. Die vertragsgemäße Nutzung des Dienstes durch den Verantwortlichen gilt als dessen Weisung.

2.2 Einzelweisungen, die nicht durch den Hauptvertrag abgedeckt sind, sind in Textform (z.B. per E-Mail) zu erteilen. Der Auftragsverarbeiter ist berechtigt, für die Bearbeitung solcher Weisungen eine angemessene Vergütung zu verlangen.

2.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere anwendbare Datenschutzvorschriften verstößt.

2.4 Der Verantwortliche weist den Auftragsverarbeiter an, aus den im Auftrag verarbeiteten

Daten nach Maßgabe von Anlage 1 anonyme, aggregierte Statistiken zu bilden. Die Anonymisierung ist Teil der weisungsgebundenen Verarbeitung. Der Auftragsverarbeiter ist berechtigt, die so entstandenen anonymen Statistiken zeitlich unbegrenzt für den sicheren Betrieb, die Fehleranalyse, die Kapazitätsplanung und die Weiterentwicklung des Dienstes zu verwenden.

2.5 Der Auftragsverarbeiter verpflichtet sich, keine Re-Identifikation zu versuchen, die Statistiken nicht an Dritte weiterzugeben, sie nicht zu Werbezwecken zu nutzen und sie nicht zum Training von KI-Modellen zu verwenden. Der Verantwortliche kann der Weisung nach Ziffer 2.4 jederzeit in Textform mit Wirkung für die Zukunft widersprechen. Der Auftragsverarbeiter nimmt die Daten des Verantwortlichen dann von der Aggregation aus; bereits gebildete anonyme Statistiken bleiben unberührt, da sie keinen Personenbezug mehr aufweisen.

§ 3 Pflichten des Auftragsverarbeiters

3.1 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.2 Unterstützung des Verantwortlichen bei Betroffenenrechten

Erhält der Auftragsverarbeiter einen Antrag einer betroffenen Person, der auf die Ausübung von Rechten gemäß Art. 12 bis 22 DSGVO gerichtet ist, leitet er diesen Antrag unverzüglich an den Verantwortlichen weiter. Der Auftragsverarbeiter wird den Verantwortlichen nach dessen Weisung mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Eine direkte Beantwortung des Antrags durch den Auftragsverarbeiter an die betroffene Person erfolgt nur mit vorheriger schriftlicher Zustimmung des Verantwortlichen oder bei Vorliegen einer gesetzlichen Verpflichtung.

3.3 Unterstützung bei weiteren Pflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im erforderlichen Umfang bei der Erfüllung seiner Pflichten nach den Artikeln 32 bis 36 DSGVO, insbesondere durch die Bereitstellung der notwendigen Informationen für eine Datenschutz-Folgenabschätzung oder für die Meldung von Datenschutzverletzungen an eine Aufsichtsbehörde. Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine angemessene Vergütung verlangen.

3.4 Rückgabe und Löschung von Daten

Nach Beendigung des Hauptvertrages hat der Verantwortliche für einen Zeitraum von 30 Tagen die Möglichkeit, seine Daten über die im Dienst bereitgestellte Exportfunktion eigenständig zu sichern. Nach Ablauf dieser Frist wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten vollständig und unwiederbringlich löschen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Der Auftragsverarbeiter wird die erfolgte Löschung auf

Anfrage des Verantwortlichen in Textform bestätigen.

§ 4 Pflichten des Verantwortlichen

4.1 Der Verantwortliche ist für die Beurteilung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten gemäß Art. 6 Abs. 1 DSGVO allein verantwortlich. Dies umfasst insbesondere die Einholung etwaig erforderlicher Einwilligungen von betroffenen Personen.

4.2 Dem Verantwortlichen obliegt die Erfüllung der Informationspflichten gemäß Art. 13 und 14 DSGVO gegenüber den betroffenen Personen.

4.3 Der Verantwortliche ist verpflichtet, die Daten, die er in den Dienst einstellt, auf ihre datenschutzrechtliche Zulässigkeit zu prüfen und seine Nutzung des Dienstes gesetzeskonform zu gestalten.

§ 5 Technische und Organisatorische Maßnahmen

5.1 Der Auftragsverarbeiter erklärt, alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau für die verarbeiteten Daten zu gewährleisten.

5.2 Die konkret getroffenen technischen und organisatorischen Maßnahmen („TOMs") sind in Anlage 2 zu diesem AVV dokumentiert. Der Verantwortliche bestätigt die in Anlage 2 dokumentierten TOMs ein angemessenes Schutzniveau für die verarbeiteten Daten bieten.

5.3 Der Auftragsverarbeiter behält sich das Recht vor, die getroffenen TOMs weiterzuentwickeln und anzupassen. Er wird dabei sicherstellen, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverhältnisse

6.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter (nachfolgend „Unterauftragsverarbeiter") zur Erbringung der vertraglichen Leistung einzusetzen.

6.2 Eine zum Zeitpunkt des Vertragsschlusses aktuelle Liste der vom Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter befindet sich in Anlage 3.

6.3 Der Auftragsverarbeiter informiert den Verantwortlichen in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Verantwortliche kann gegen eine solche Änderung innerhalb von zwei Wochen nach Zugang der Information aus einem wichtigen, datenschutzrechtlichen Grund schriftlich Widerspruch einlegen. Liegt kein Widerspruch innerhalb der Frist vor, gilt die Änderung als genehmigt.

6.4 Im Falle eines berechtigten Widerspruchs ist der Auftragsverarbeiter berechtigt, den Dienst ohne Einsatz des geplanten Unterauftragsverarbeiters weiter zu erbringen oder den Hauptvertrag mit einer angemessenen Frist außerordentlich zu kündigen.

6.5 Der Auftragsverarbeiter schließt mit den Unterauftragsverarbeitern die erforderlichen Verträge gemäß Art. 28 Abs. 4 DSGVO ab und stellt sicher, dass diese den Unterauftragsverarbeitern im Wesentlichen die gleichen Datenschutzpflichten auferlegen, die für den Auftragsverarbeiter selbst gelten.

6.6 Eine Übermittlung von im Auftrag verarbeiteten Daten in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittland) durch den Auftragsverarbeiter oder seine Unterauftragsverarbeiter ist nur zulässig, soweit die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 7 Kontroll- und Auditrechte des Verantwortlichen

7.1 Der Verantwortliche hat das Recht, sich von der Einhaltung der in diesem AVV getroffenen Regelungen zu überzeugen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen die dafür erforderlichen Informationen zur Verfügung zu stellen.

7.2 Der Auftragsverarbeiter kann den Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen insbesondere durch die Vorlage von Dokumentation, Testaten, Berichten unabhängiger Prüfer oder geeigneten Zertifizierungen erbringen.

7.3 Eine Inspektion vor Ort durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer ist nur zulässig soweit a) die vom Auftragsverarbeiter gemäß Ziffer 7.2 vorgelegten Nachweise sich als nicht ausreichend erweisen, um die Einhaltung der Pflichten darzulegen, oder b) es liegt ein schwerwiegender, den Verantwortlichen betreffender und nachgewiesener Datenschutzvorfall beim Auftragsverarbeiter vor. Die Inspektion ist auf den konkreten Anlass zu beschränken und nach rechtzeitiger Ankündigung (in der Regel mindestens vier Wochen) während der üblichen Geschäftszeiten und unter strenger Wahrung der Betriebsabläufe und Geschäftsgeheimnisse durchzuführen. Der Verantwortliche trägt sämtliche Kosten der Inspektion, einschließlich des internen Aufwands des Auftragsverarbeiters. Das Recht zur Inspektion ist grundsätzlich auf ein Mal pro Kalenderjahr beschränkt.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

8.1. Der Auftragsverarbeiter meldet dem Verantwortlichen unverzüglich jede Verletzung des Schutzes personenbezogener Daten, die die im Auftrag dieses Verantwortlichen verarbeiteten Daten betrifft, nachdem ihm diese bekannt geworden ist. Die Meldung erfolgt unter Beachtung der Anforderungen des Art. 33 Abs. 3 DSGVO, soweit die Informationen für den Auftragsverarbeiter verfügbar sind.

8.2. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen eigenen Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO) im angemessenen Rahmen. Soweit es nicht möglich ist, alle Informationen zur Datenschutzverletzung gleichzeitig bereitzustellen, wird der Auftragsverarbeiter den Verantwortlichen ohne unangemessene weitere Verzögerung schrittweise informieren, sobald die jeweiligen Erkenntnisse vorliegen.

§ 9 Haftung

Für die Haftung der Parteien bei Datenschutzverstößen gilt Art. 82 DSGVO. Im Innenverhältnis der Parteien gelten die im Hauptvertrag vereinbarte Haftung.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Absatz 4 bleibt unberührt.

(2) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Dieser AVV findet deutsches Recht Anwendung. Anwendbares Recht sowie der ausschließliche Gerichtsstand unterliegen der Regelungen des Hauptvertrages.

(4) Dieser AVV wird elektronisch abgeschlossen: Der Verantwortliche stimmt dem AVV im Rahmen des Bestellprozesses (Checkout) bzw. im Nutzerkonto ausdrücklich zu; die Zustimmung wird vom Auftragsverarbeiter protokolliert. Einer Unterschrift der Parteien bedarf es nicht. Auf Verlangen stellt der Auftragsverarbeiter eine von der Geschäftsführung gezeichnete Fassung bereit.

Anlage 1: Spezifikation der Auftragsverarbeitung

1. Art und Zweck der Verarbeitung:

- Erbringung des SaaS-Dienstes "MeetEffX" als KI-gestützter Meeting-Coach.
- Zwecke: Vorbereitung, Durchführung und Analyse von Meetings; Erstellung von Aktionspunkten; Analyse von Interaktionsmustern, Persönlichkeitstypen und Synergien zur Optimierung der Zusammenarbeit ausschließlich innerhalb des Accounts des jeweiligen Kunden.
- Zusätzlicher Zweck: Erzeugung anonymer, aggregierter Nutzungs- und Betriebsstatistiken über Art, Umfang und technische Qualität der Nutzung des Dienstes. Die Aggregation erfolgt ausschließlich auf Systemen des Auftragsverarbeiters innerhalb der Europäischen Union. In die Statistiken fließen keine Meeting-Inhalte, keine Klarnamen, keine Kontaktdaten und keine Ergebnisse der Persönlichkeits- oder Stimmungsanalyse ein. Eine Statistikzelle wird nur gebildet und gespeichert, wenn mindestens fünf verschiedene Verantwortliche zu ihr beitragen.

2. Art der personenbezogenen Daten, die im Auftrag verarbeitet werden:

- Teilnehmer-Stammdaten: Name, E-Mail-Adresse von durch den Kunden eingeladenen Teilnehmern.
- Meeting-Inhalte: Agenden, Notizen, Kommentare, Aufgaben, Protokolle und andere vom Kunden oder Teilnehmern eingegebene Inhalte. Audio- und Video-Signale werden ausschließlich lokal auf dem Endgerät des jeweiligen Nutzers analysiert; rohe Audio- oder Video-Daten werden nicht an den Auftragsverarbeiter übertragen oder von ihm gespeichert – übermittelt werden nur aggregierte Kennzahlen (siehe Meeting-Metadaten).
- Meeting-Metadaten: Analysedaten wie Redeanteile, Interaktionsmuster, Sentiment-Analysen.
- Freiwillige Zusatzdaten: Ergebnisse aus Angaben zur Ermittlung von Persönlichkeitstypen.
- Kreis der betroffenen Personen: Mitarbeiter, Berater, Kunden und sonstige Geschäftspartner des Verantwortlichen, die als Teilnehmer zu Meetings eingeladen werden.

Anlage 2: Technische und Organisatorische Maßnahmen gemäß Art. 32 DSGVO

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

- Verschlüsselung: Sämtliche Datenübertragungen erfolgen TLS-verschlüsselt (HTTPS mit automatisierter Zertifikatsverwaltung); interne Dienste sind nicht öffentlich exponiert. Die Anwendungsdatenbank ist bei der Speicherung (at rest) verschlüsselt (Managed PostgreSQL); Kalender-/OAuth-Tokens werden zusätzlich anwendungsseitig verschlüsselt gespeichert.
- Pseudonymisierung/Anonymisierung: Passwörter werden ausschließlich als Hash im selbst betriebenen Identity-Provider (Keycloak) gespeichert. Ein Lösch- und Anonymisierungskonzept kappt auf Antrag den Personenbezug (Anonymisierung referenzierter Datensätze, harte Löschung rein persönlicher Daten).

2. Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)

- Vertraulichkeit:

- Zutrittskontrolle: Betrieb ausschließlich in ISO-27001-zertifizierten Rechenzentren in Deutschland (Hetzner) bzw. in der EU-Region Frankfurt (Datenbank) mit professioneller physischer Zutrittssicherung; ein physischer Serverzugang durch den Auftragsverarbeiter ist nicht erforderlich.
- Zugangskontrolle: Administrativer Serverzugriff ausschließlich schlüsselbasiert per SSH für benannte Administratoren; Secrets werden serverseitig mit restriktiven Dateirechten verwaltet, CI/CD-Zugänge über geschützte Repository-Secrets. Die Anwendung nutzt eine zentrale Authentifizierung über ein selbst betriebenes Keycloak (token-basierte Sessions, Passwörter nur als Hash).
- Zugriffskontrolle: Rollenbasiertes Berechtigungskonzept (Owner/Admin/Mitglied bzw. Moderator/Teilnehmer); logische Mandantentrennung der Kundendaten auf Datenbankebene durch Row-Level-Security (RLS); mandantengebundene Zugriffe werden in der API erzwungen.

- Integrität:

- Weitergabekontrolle: TLS-Verschlüsselung für sämtliche Übertragungswege; die Übermittlung an den KI-Anbieter (EU) ist auf die für die jeweilige Funktion erforderlichen Meeting-Inhalte beschränkt; kein Einsatz von Tracking- oder Werbe-Tools Dritter in der Anwendung; keine Erstellung von Nutzungsprofilen einzelner Teilnehmer. Die eigene, serverseitige Betriebsmessung des Auftragsverarbeiters ohne Zugriff auf Endgeräte bleibt nach Maßgabe von § 2.4, § 2.5 und Anlage 1 zulässig.
- Eingabekontrolle: Audit-Logging sicherheits- und datenschutzrelevanter Ereignisse (u. a. Anmeldungen, Berechtigungs- und Einwilligungsänderungen) mit definierten Aufbewahrungsfristen.

- Verfügbarkeit und Belastbarkeit:

- Automatisierte, regelmäßige Datenbank-Backups; redundante Systemauslegung beim Rechenzentrumsbetreiber; Fehler- und Crash-Monitoring über eine selbst gehostete Monitoring-Lösung (GlitchTip) ohne Weitergabe an externe Monitoring-Clouds.

- Dokumentiertes Wiederherstellungs- und Rollback-Verfahren für Deployments; automatisierte Health-Checks und Smoke-Tests im Deploy-Prozess.

3. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO)

- Automatisierte, protokollierte Lösch- und Aufräumprozesse (Retention) mit definierten Fristen; Self-Service-Datenexport und Löschantrag mit Doppelbestätigung im Datenschutz-Center; Änderungen an Infrastruktur und Sicherheitsmaßnahmen werden versioniert dokumentiert (Repository/Runbook); regelmäßige interne Überprüfung der Sicherheits- und Datenschutzkonzepte.

Anlage 3: Genehmigte Unterauftragsverarbeiter

Unternehmen & Sitz · Beschreibung der Leistung · Ort der Verarbeitung

Hetzner Online GmbH, Deutschland · Hosting der Anwendungsserver und -infrastruktur · Deutschland

Sendinblue GmbH (Brevo), Deutschland · Versand von Transaktions-/System-E-Mails und Einladungen · Deutschland / EU

Neon, Inc., USA · Hosting der Anwendungsdatenbank · EU-Region Frankfurt (Deutschland); Anbietersitz USA – EU-Standardvertragsklauseln vereinbart

Mistral AI, SAS, Frankreich · Bereitstellung des KI-Sprachmodells zur Analyse · Frankreich