

Auftragsverarbeitungsvertrag (AVV)

Stand: 25.10.2026

Online-Fassung: <https://vertriebs-ai.de/avv>

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) gilt für alle Kunden der MW Software GbR, die die Plattform vertriebs-ai.de nutzen. Er ergänzt den Vertrag, den der Kunde auf Grundlage der Nutzungsbedingungen mit der MW Software GbR schließt (nachfolgend „Nutzungsvertrag“), und wird mit dessen Abschluss Vertragsbestandteil.

Auftragsverarbeiter

MW Software GbR
Hinschstr. 18, 22525 Hamburg, Deutschland
E-Mail: info@vertriebs-ai.de
vertreten durch Philipp Meyer

nachfolgend „Auftragsverarbeiter“ oder „Vertriebs AI“

Verantwortlicher

Der jeweilige Kunde gemäß geschlossenem Nutzungsvertrag mit der MW Software GbR

nachfolgend „Verantwortlicher“ oder „Kunde“, gemeinsam mit dem Auftragsverarbeiter die „Parteien“

1. Präambel

- (1) Der Auftragsverarbeiter stellt dem Kunden unter der Marke vertriebs-ai.de eine Software-Plattform für KI-gestütztes Verkaufstraining, insbesondere für realistische Telefonsimulationen, Gesprächsauswertungen, Team-Management, Bewertungsbögen und zugehörige Analysefunktionen, als SaaS-Lösung bereit.
- (2) Soweit der Auftragsverarbeiter im Rahmen der Leistungserbringung personenbezogene Daten im Auftrag des Kunden verarbeitet, gilt dieser AVV gemäß Art. 28 DSGVO. Er wird mit Abschluss des Nutzungsvertrags vereinbart: bei kostenpflichtigen Verträgen mit der Annahme des Angebots durch einen hierzu befugten Vertreter des Kunden, bei einer kostenlosen Testphase mit der Annahme der Nutzungsbedingungen bei der Einrichtung der Testphase für das Unternehmen. Nutzerkonten, die der Kunde für seine Beschäftigten anlegt oder zu denen er sie einlädt, begründen keinen eigenen AVV.
- (3) Dieser AVV konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit den vom Auftragsverarbeiter für den Kunden vorgenommenen Verarbeitungsvorgängen.

2. Gegenstand und Dauer der Verarbeitung

- (1) Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Zusammenhang mit der Bereitstellung und dem Betrieb der Plattform sowie der damit verbundenen Support-, Hosting-, Analyse- und Verwaltungsleistungen.
- (2) Die Einzelheiten zu Gegenstand, Art und Zweck der Verarbeitung, den Datenarten, den Kategorien betroffener Personen sowie den konkreten Verarbeitungstätigkeiten ergeben sich aus [Anlage 1](#).
- (3) Die Verarbeitung beginnt mit Inkrafttreten des Nutzungsvertrags zwischen den Parteien oder mit erstmaliger Nutzung der Leistungen des Auftragsverarbeiters durch den Kunden, je nachdem, was früher eintritt.
- (4) Die Laufzeit dieses AVV richtet sich nach der Laufzeit des Nutzungsvertrags. Dieser AVV endet automatisch mit Beendigung des Nutzungsvertrags, sofern nicht gesetzliche Aufbewahrungspflichten oder die Regelungen dieses AVV eine darüber hinausgehende Verarbeitung oder Speicherung erfordern.

3. Art, Zweck und Umfang der Verarbeitung

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich geschuldeten Leistungen für den Kunden.
- (2) Die Verarbeitung umfasst insbesondere:
 - Bereitstellung von Benutzerkonten und Organisationsstrukturen
 - Speicherung und Verwaltung kundenseitig eingegebener Inhalte
 - Durchführung und Dokumentation von Trainingsgesprächen
 - Speicherung und Verarbeitung von Gesprächsmetadaten, Transkripten und Auswertungen
 - Automatisierte Analyse von Gesprächsinhalten zur Bereitstellung von Feedback- und Coaching-Funktionen
 - Abwicklung technischer Administration, Support- und Sicherheitsmaßnahmen
 - Protokollierung sicherheits- und administrationsbezogener Ereignisse
- (3) Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters erfolgt nicht, soweit in diesem AVV oder im Nutzungsvertrag nicht ausdrücklich etwas anderes geregelt ist oder hierfür eine eigenständige datenschutzrechtliche Verantwortlichkeit des Auftragsverarbeiters besteht.
- (4) Die Verarbeitung dient ausschließlich dem Trainingszweck im Sinne der Ziffer 6.2 der Nutzungsbedingungen. Eine Verarbeitung zur Überwachung oder Bewertung der beruflichen Leistung oder des Verhaltens von Beschäftigten außerhalb des Trainingszwecks oder zur Vorbereitung von Entscheidungen über Beschäftigungsverhältnisse ist nicht Gegenstand der vertraglich geschuldeten Leistung. Weisungen, die auf eine solche Verarbeitung gerichtet sind, sind von diesem AVV nicht gedeckt.

4. Weisungsrecht des Verantwortlichen

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden im Sinne des Art. 28 Abs. 3 lit. a DSGVO, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragsverarbeiter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.
- (2) Als dokumentierte Weisungen gelten:
 - die Bestimmungen dieses AVV
 - der Nutzungsvertrag einschließlich Leistungsbeschreibung
 - die vom Kunden in der Plattform vorgenommenen Konfigurationen und Einstellungen
 - schriftliche oder in Textform erteilte Einzelweisungen des Kunden
- (3) Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
- (4) Hält der Auftragsverarbeiter eine Weisung des Kunden für datenschutzrechtlich unzulässig, wird er den Kunden unverzüglich darauf hinweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch den Kunden auszusetzen.

5. Pflichten des Auftragsverarbeiters

- (1)

Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten nur im Rahmen der Weisungen des Kunden und der vertraglichen Vereinbarungen zu verarbeiten.

- (2) Der Auftragsverarbeiter gewährleistet, dass alle mit der Verarbeitung personenbezogener Daten befassten Personen:
 - zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen
 - nur in dem Umfang Zugriff auf personenbezogene Daten erhalten, wie dies für die Erfüllung ihrer Aufgaben erforderlich ist
 - regelmäßig zum Datenschutz und zur Informationssicherheit sensibilisiert werden
- (3) Der Auftragsverarbeiter trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt der Veröffentlichung dieses AVV bestehenden Maßnahmen sind in [Anlage 2](#) beschrieben.
- (4) Der Auftragsverarbeiter unterstützt den Kunden im Rahmen des Zumutbaren und unter Berücksichtigung der Art der Verarbeitung bei der Erfüllung der datenschutzrechtlichen Pflichten des Kunden, insbesondere bei:
 - der Wahrnehmung von Betroffenenrechten
 - der Sicherstellung der Sicherheit der Verarbeitung
 - Meldungen von Verletzungen des Schutzes personenbezogener Daten
 - Datenschutz-Folgenabschätzungen
 - etwaigen Konsultationen mit Aufsichtsbehörden
- (5) Der Auftragsverarbeiter informiert den Kunden unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die personenbezogene Daten betrifft, die im Auftrag des Kunden verarbeitet werden.
- (6) Der Auftragsverarbeiter führt ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO, soweit gesetzlich erforderlich.

6. Pflichten des Verantwortlichen

- (1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.
- (2) Der Kunde versichert, dass er alle personenbezogenen Daten, die er über die Plattform verarbeiten lässt, rechtmäßig erhoben hat und deren Verarbeitung über die Plattform datenschutzrechtlich zulässig ist.
- (3) Der Kunde ist insbesondere verantwortlich für:
 - die Auswahl und Zulässigkeit der von ihm eingegebenen Inhalte
 - die Erfüllung eigener Informationspflichten gegenüber betroffenen Personen
 - die Prüfung einer etwaigen Erforderlichkeit von Einwilligungen, Betriebsvereinbarungen oder sonstigen Rechtsgrundlagen
 - die Prüfung, ob besondere Kategorien personenbezogener Daten verarbeitet werden dürfen
 - die Einhaltung der Zweckbindung nach Ziffer 3 Abs. 4 durch seine Nutzer, insbesondere durch Administratoren und Führungskräfte

- (4) Der Kunde wird den Auftragsverarbeiter unverzüglich informieren, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit datenschutzrechtlichen Anforderungen feststellt.

7. Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter implementiert und unterhält geeignete technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- (2) Die bei Veröffentlichung dieses AVV bestehenden Maßnahmen ergeben sich aus [Anlage 2](#). Der Auftragsverarbeiter ist berechtigt, diese Maßnahmen weiterzuentwickeln oder zu ändern, sofern das Sicherheitsniveau nicht unterschritten wird.
- (3) Wesentliche Änderungen, die das Schutzniveau beeinflussen können, werden dem Kunden rechtzeitig mitgeteilt, z. B. per E-Mail oder durch Aktualisierung dieses AVV.

8. Unterstützung bei Betroffenenrechten

- (1) Der Auftragsverarbeiter unterstützt den Kunden durch geeignete technische und organisatorische Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen, soweit dies unter Berücksichtigung der Art der Verarbeitung möglich ist.
- (2) Geht beim Auftragsverarbeiter ein Antrag einer betroffenen Person ein, der sich erkennbar auf Daten des Kunden bezieht, wird der Auftragsverarbeiter diesen Antrag unverzüglich an den Kunden weiterleiten, sofern eine eigenständige Bearbeitung durch den Auftragsverarbeiter gesetzlich nicht erforderlich ist.
- (3) Eine unmittelbare Beantwortung gegenüber der betroffenen Person erfolgt durch den Auftragsverarbeiter nur nach dokumentierter Weisung des Kunden oder soweit eine gesetzliche Verpflichtung hierzu besteht.

9. Meldung von Datenschutzvorfällen

- (1) Der Auftragsverarbeiter informiert den Kunden unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, soweit Daten betroffen sind, die der Auftragsverarbeiter im Auftrag des Kunden verarbeitet.
- (2) Die Mitteilung enthält, soweit zum Zeitpunkt der Meldung verfügbar:
- eine Beschreibung der Art des Vorfalls
 - die betroffenen Datenkategorien und Personengruppen
 - die wahrscheinlichen Folgen
 - die bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Eindämmung und Abhilfe
 - eine Kontaktmöglichkeit für Rückfragen
- (3) Der Auftragsverarbeiter unterstützt den Kunden im angemessenen Umfang bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

10. Nachweis und Kontrollrechte

- (1) Der Auftragsverarbeiter stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten nachzuweisen.
- (2) Der Kunde ist berechtigt, die Einhaltung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter nach angemessener Vorankündigung (mindestens 14 Tage) während der üblichen

Geschäftszeiten zu überprüfen oder durch einen zur Verschwiegenheit verpflichteten Dritten überprüfen zu lassen, sofern hierfür ein berechtigter Anlass besteht.

- (3) Vor-Ort-Kontrollen sind auf das erforderliche Maß zu beschränken und so durchzuführen, dass Betriebs- und Geschäftsabläufe des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigt werden und keine Rechte Dritter oder Geschäftsgeheimnisse gefährdet werden.
- (4) Sofern dem Kunden geeignete aktuelle Nachweise, Prüfberichte, Zertifizierungen oder Selbstauskünfte zur Verfügung gestellt werden und diese den berechtigten Prüfzweck angemessen erfüllen, kann der Auftragsverarbeiter verlangen, dass diese vorrangig genutzt werden.

11. Unterauftragsverhältnisse

- (1) Der Kunde erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO einzusetzen, soweit dies zur Leistungserbringung erforderlich ist.
- (2) Die zum Zeitpunkt der Veröffentlichung dieses AVV eingesetzten Unterauftragsverarbeiter ergeben sich aus [Anlage 3](#).
- (3) Der Auftragsverarbeiter wird den Kunden über jede beabsichtigte Hinzuziehung neuer oder den Austausch bestehender Unterauftragsverarbeiter rechtzeitig vorab informieren, z. B. per E-Mail oder durch Aktualisierung dieses AVV. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund binnen 14 Kalendertagen ab Zugang der Information widersprechen.
- (4) Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt.
- (5) Im Fall eines begründeten Widerspruchs werden die Parteien prüfen, ob eine für beide Seiten zumutbare Alternative besteht. Besteht keine zumutbare Alternative, sind beide Parteien berechtigt, den betroffenen Teil der Leistungen oder den Nutzungsvertrag mit angemessener Frist außerordentlich zu kündigen.
- (6) Der Auftragsverarbeiter stellt sicher, dass mit jedem Unterauftragsverarbeiter ein Vertrag geschlossen wird, der im Wesentlichen dieselben Datenschutzpflichten enthält, die in diesem AVV vereinbart sind.
- (7) Der Auftragsverarbeiter bleibt dem Kunden gegenüber für die Erfüllung der Pflichten der Unterauftragsverarbeiter verantwortlich.

12. Verarbeitung in Drittstaaten

- (1) Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO eingehalten sind.
- (2) Soweit Unterauftragsverarbeiter in Drittstaaten eingesetzt werden oder ein Zugriff aus Drittstaaten nicht ausgeschlossen werden kann, stellt der Auftragsverarbeiter sicher, dass hierfür ein zulässiger Transfermechanismus besteht, insbesondere ein Angemessenheitsbeschluss oder geeignete Garantien wie Standardvertragsklauseln.
- (3) Informationen zu relevanten Drittstaatentransfers ergeben sich aus [Anlage 3](#).

13. Löschung und Rückgabe von Daten

- (1) Nach Beendigung des Nutzungsvertrags wird der Auftragsverarbeiter nach Wahl des Kunden sämtliche personenbezogene Daten, die im Auftrag verarbeitet wurden, entweder löschen oder an den Kunden zurückgeben, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.
- (2)

Soweit gesetzliche Aufbewahrungspflichten bestehen, wird der Auftragsverarbeiter die betroffenen Daten für die Dauer der gesetzlichen Aufbewahrungspflicht weiter speichern und ihre Verarbeitung auf diesen Zweck beschränken.

- (3) Der Kunde hat sein Wahlrecht nach Absatz 1 spätestens innerhalb von 30 Kalendertagen nach Vertragsende in Textform auszuüben. Erfolgt keine fristgerechte Erklärung, ist der Auftragsverarbeiter berechtigt, die Daten datenschutzkonform zu löschen.
- (4) Bereits während der Laufzeit des Nutzungsvertrags kann der Kunde in Textform eine Löschfrist für Gesprächsdaten von 30, 90, 180 oder 365 Tagen anweisen. Der Auftragsverarbeiter löscht dann Gespräche, Transkripte, Auswertungen, Coach-Chats und die zugehörigen personenbezogenen Werte der Organisation automatisch nach Ablauf der Frist. Maßgeblich ist der Zeitpunkt des Gesprächs, bei hochgeladenen echten Gesprächen der Zeitpunkt des Uploads. Die Löschläufe sind für berechtigte Administratoren des Kunden in den Datenschutz-Einstellungen der Organisation einsehbar.

14. Vertraulichkeit und Geheimnisschutz

- (1) Die Parteien behandeln alle im Zusammenhang mit diesem AVV erlangten vertraulichen Informationen vertraulich.
- (2) Kontroll- und Auditmaßnahmen des Kunden dürfen nicht dazu führen, dass Geschäftsgeheimnisse, sicherheitsrelevante Informationen oder Daten anderer Kunden des Auftragsverarbeiters offengelegt werden.

15. Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften sowie den Haftungsregelungen des Nutzungsvertrags. Zwingende Haftungsregelungen der DSGVO, insbesondere Art. 82 DSGVO, bleiben unberührt.

16. Schlussbestimmungen

- (1) Dieser AVV ist Bestandteil des Nutzungsvertrags zwischen den Parteien. Bei Widersprüchen gehen hinsichtlich des Datenschutzes die Regelungen dieses AVV vor.
- (2) Änderungen und Ergänzungen dieses AVV bedürfen einer Vereinbarung der Parteien in Textform; Schweigen gilt nicht als Zustimmung. Unberührt bleiben die Information über neue oder ausgetauschte Unterauftragsverarbeiter mit Widerspruchsrecht nach Ziffer 11 sowie die Weiterentwicklung der technischen und organisatorischen Maßnahmen nach Ziffer 7, soweit das Schutzniveau nicht unterschritten wird.
- (3) Sollten einzelne Bestimmungen dieses AVV ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (4) Dieser AVV wird nach Ziffer 1 Abs. 2 vereinbart und in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Eine gesonderte Unterschrift ist nicht erforderlich. Auf Wunsch stellt der Auftragsverarbeiter dem Kunden eine unterzeichnete Fassung zur Verfügung.

Anlage 1 – Beschreibung der Verarbeitung

1. Gegenstand der Auftragsverarbeitung

Bereitstellung und Betrieb einer cloudbasierten Plattform für KI-gestütztes Verkaufstraining einschließlich Nutzerverwaltung, Organisations- und Teamfunktionen, Gesprächsdurchführung, Gesprächsdokumentation, Gesprächsauswertung, Bereitstellung von Scorecards, Coaching-Funktionen, Reporting- und Administrationsfunktionen sowie technischem Support.

2. Art und Zweck der Verarbeitung

Die Verarbeitung dient insbesondere folgenden Zwecken:

- Einrichtung und Verwaltung von Benutzerkonten
- Durchführung von KI-basierten Trainingsgesprächen
- Erstellung, Speicherung und Auswertung von Gesprächsprotokollen und Transkripten
- Erzeugung von KI-gestütztem Feedback und Coaching-Auswertungen
- Verwaltung von Teams, Rollen, Berechtigungen und Organisationseinheiten
- Dokumentation administrativer und sicherheitsbezogener Ereignisse
- Bereitstellung von Support- und Fehleranalysefunktionen
- Abrechnung und Verwaltung gebuchter Leistungen, soweit personenbezogene Daten des Kunden betroffen sind

Die Verarbeitung dient nicht der Überwachung oder Bewertung der beruflichen Leistung oder des Verhaltens von Beschäftigten und nicht der Vorbereitung von Entscheidungen über Beschäftigungsverhältnisse (Zweckbindung nach Ziffer 3 Abs. 4 dieses AVV und Ziffer 6.2 der Nutzungsbedingungen).

3. Kategorien betroffener Personen

Je nach Nutzung der Plattform können insbesondere folgende Personengruppen betroffen sein:

- Mitarbeitende des Kunden
- Administratoren und Teamleiter des Kunden
- Trainer, Coaches oder sonstige vom Kunden autorisierte Nutzer
- Ansprechpartner des Kunden
- Personen, deren personenbezogene Daten durch den Kunden in Trainingsszenarien, Transkripten, Notizen oder Organisationsdaten verarbeitet werden

4. Arten personenbezogener Daten

Je nach Nutzung und Konfiguration der Plattform können insbesondere folgende Daten verarbeitet werden:

- Stammdaten (z. B. Name, E-Mail-Adresse, Rollen- und Organisationszuordnung)
- Kontaktdaten
- Authentifizierungs- und Accountdaten
- Kommunikations- und Nutzungsdaten
- Gesprächsmetadaten (z. B. Zeitpunkt, Dauer, technische Sessiondaten)
- Gesprächsinhalte und Transkripte
- Vom Kunden erstellte Profile, Scorecards, Notizen und Bewertungsdaten
- Analyse- und Feedbackdaten
- Abrechnungs- und Vertragsdaten
- Protokoll- und Auditdaten mit Personenbezug

5. Besondere Kategorien personenbezogener Daten

Eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ist nicht vorgesehen und soll durch den Kunden grundsätzlich vermieden werden. Soweit der Kunde dennoch entsprechende Daten übermitteln oder verarbeiten lassen möchte, ist allein der Kunde dafür verantwortlich, dass hierfür eine geeignete Rechtsgrundlage besteht und der Auftragsverarbeiter hierüber vorab informiert wurde.

6. Häufigkeit und Umfang

Die Verarbeitung erfolgt fortlaufend, wiederkehrend und nach Maßgabe der Nutzung der Plattform durch den Kunden.

7. Ort der Verarbeitung

Die Verarbeitung erfolgt primär innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Einzelne Drittlandbezüge können sich aus den in [Anlage 3](#) genannten Unterauftragsverarbeitern oder deren Konzernstrukturen ergeben.

8. Abgrenzung der Verantwortlichkeiten

Nicht jede Datenverarbeitung im Umfeld der Geschäftsbeziehung fällt unter diesen AVV. Verarbeitungen, bei denen Vertriebs AI eigenständiger Verantwortlicher ist, bleiben unberührt. Hierzu gehören insbesondere:

- Verarbeitung von Kontakt- und Vertragsdaten zur eigenen Vertragsverwaltung
- Rechnungsstellung, Buchhaltung und steuerrechtliche Pflichten
- Eigene Sicherheits- und Missbrauchspräventionsinteressen
- Eigene Marketing- und Vertriebsprozesse von Vertriebs AI
- Gesetzlich verpflichtende Offenlegungen oder Nachweise

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

Die nachfolgenden Maßnahmen beschreiben das zum Zeitpunkt der Veröffentlichung dieses AVV bestehende Sicherheitsniveau. Der Auftragsverarbeiter darf die Maßnahmen fortentwickeln, sofern das Schutzniveau nicht unterschritten wird.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Zutritt zu produktionsrelevanten Systemen nur für autorisierte Personen
- Nutzung etablierter Cloud-Infrastrukturen mit physischen Sicherheitsmaßnahmen des jeweiligen Hosting-Anbieters

1.2 Zugangskontrolle

- Zugriff auf Administrations- und Produktivsysteme nach Berechtigungskonzept
- Verwendung individueller Benutzerkennungen
- Multifaktorauthentifizierung für interne Zugänge, soweit verfügbar und vorgesehen
- Starke Passwortrichtlinien und Zugriffsbeschränkungen für privilegierte Konten

1.3 Zugriffskontrolle

- Rollen- und berechtigungsbasierte Zugriffskonzepte

- Beschränkung des Datenzugriffs nach Need-to-know-Prinzip
- Begrenzte Administrator-Konten
- Trennung von regulären Nutzer- und Administrationsrechten

1.4 Weitergabekontrolle

- Transportverschlüsselung für Datenübertragungen (TLS, mindestens Version 1.2)
- Absicherung externer Schnittstellen und API-Zugriffe
- Drittlandtransfers nur unter Beachtung der Art. 44 ff. DSGVO

1.5 Eingabekontrolle

- Protokollierung relevanter administrativer und sicherheitsbezogener Vorgänge
- Audit-Logging für ausgewählte organisationsbezogene Aktionen
- Nachvollziehbarkeit von Änderungen im Rahmen technischer Protokolle

2. Integrität

- Schutz vor unbefugter Veränderung durch Berechtigungs- und Rollenkonzepte
- Validierungs- und Plausibilisierungsmechanismen in Anwendungs- und Backend-Prozessen
- Teilweise manipulationsnachweisbare Audit-Protokollierung für sicherheitsrelevante Organisationsereignisse

3. Verfügbarkeit und Belastbarkeit

- Betrieb auf skalierbarer Cloud-Infrastruktur
- Maßnahmen zur Systemstabilität, Fehlererkennung und Wiederherstellbarkeit
- Protokollierung technischer Fehler und sicherheitsrelevanter Ereignisse
- Schutzmechanismen gegen Missbrauch und Überlastung im üblichen Betriebsrahmen

4. Verschlüsselung

- Transportverschlüsselung aller Verbindungen mit TLS (mindestens Version 1.2)
- Verschlüsselung gespeicherter Daten mit AES-256 auf Infrastruktur- und Plattformebene (gemäß eingesetztem Cloud-Anbieter)

5. Belastbarkeit und Wiederherstellung

- Einsatz von Cloud-Diensten mit Mechanismen zur Redundanz und Ausfallsicherheit
- Regelmäßige Aktualisierung und Wartung der produktiven Umgebung
- Wiederanlauf und Wiederherstellung im Rahmen der Möglichkeiten der eingesetzten Cloud- und Plattformanbieter

6. Verfahren zur regelmäßigen Überprüfung

- Laufende technische Weiterentwicklung der Sicherheitsmaßnahmen

- Prüfung von Zugriffsrechten und internen Berechtigungen nach Bedarf
- Fehler- und Ereignisüberwachung
- Tests und Qualitätssicherungsmaßnahmen im Rahmen des Entwicklungs- und Release-Prozesses

7. Trennung

- Logische Trennung von Kundendaten über Mandanten-, Organisations- und Rechtekonzepte innerhalb der Anwendung
- Getrennte Verarbeitungskontexte für Entwicklungs-, Test- und Produktivumgebungen, soweit betrieblich vorgesehen

8. Unterstützung bei Betroffenenrechten und Löschung

- Möglichkeiten zur Löschung oder Sperrung von Nutzerkonten und zugehörigen Daten im Rahmen der Produktfunktionen und Backend-Prozesse
- Unterstützung bei Datenexporten, Korrekturen oder Löschungen im Rahmen technischer Möglichkeiten und der vertraglichen Vereinbarungen

Anlage 3 – Unterauftragsverarbeiter

Diese Übersicht zeigt, welche Drittanbieter (Unterauftragsverarbeiter) im Rahmen der Nutzung von Vertriebs AI personenbezogene Daten im Auftrag verarbeiten. Stand: 25.10.2026.

Name des Anbieters	Zweck der Verarbeitung	Verarbeitungsort	Rechtsgrundlage der Übermittlung
Microsoft Ireland Operations Ltd.	KI-Analyse von Verkaufsgesprächen (Azure OpenAI)	Deutschland (Region: Germany West Central, Frankfurt am Main); Verarbeitung innerhalb der EU-Datenzone	DPA + SCC / Hosting in der EU
Microsoft Ireland Operations Ltd.	Textextraktion aus hochgeladenen Dokumenten (Azure Content Understanding)	Schweden (Region: Sweden Central); Verarbeitung innerhalb der EU-Datenzone	DPA + SCC / Hosting in der EU
Google Ireland Limited	Backend-Infrastruktur, Hosting, Datenbank, Dateispeicher, Nutzer-Authentifizierung (Firebase/Google Cloud), Audit-Protokoll (BigQuery)	Deutschland (Datenbank, Dateispeicher, Audit-Protokoll: Frankfurt am Main), Belgien (Backend-Funktionen), Niederlande (Hosting); Nutzer-Authentifizierung standortübergreifend, auch USA	DPA + SCC / EU-U.S. Data Privacy Framework
Google Ireland Limited	E-Mail & Kollaboration (Google Workspace)	EU	DPA + SCC / EU-U.S. Data Privacy Framework

ElevenLabs Inc.	KI-Sprachsynthese (Text-to-Speech) & Conversational AI, Spracherkennung hochgeladener Gesprächsaufnahmen	EU Data Residency; Verarbeitung durch Unterauftragnehmer sowie Zugriffe durch Support- und Moderationsteams außerhalb der EU möglich	DPA + Standardvertragsklauseln (SCC)
Sendinblue GmbH (Brevo)	E-Mail-Versand (transaktional & Marketing)	Deutschland	DPA (Serverstandort Deutschland)
PostHog Inc. (USA)	Produkt- & Nutzungs-Analytics	Deutschland (EU-Cloud, Frankfurt am Main)	DPA + SCC / EU-U.S. Data Privacy Framework
Stripe Payments Europe, Ltd.	Abwicklung von Online-Zahlungen	Irland (EU) und USA (Stripe, LLC)	DPA + SCC / EU-U.S. Data Privacy Framework
Slack Technologies Limited	Interne Benachrichtigungen (Testphasen, Vertragseignisse, Kundenbetreuung, gemeldete KI-Auswertungen)	Irland (EU) und USA	DPA + SCC / EU-U.S. Data Privacy Framework
Twilio Ireland Limited	Telefonie für eingehende Trainingsanrufe	EU (Irland, Region IE1); Konto-, Abrechnungs- und Verwaltungsdaten auch USA	DPA + Binding Corporate Rules / EU-U.S. Data Privacy Framework
HubSpot Ireland Limited	CRM, Lead-Management & Kundensupport	Irland (EU)	DPA + SCC

Erläuterungen zu den Rechtsgrundlagen

DPA	Data Processing Agreement: Mit allen oben genannten Anbietern wurde ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO abgeschlossen.
SCC	Standard Contractual Clauses: Für Übermittlungen in Drittländer (z. B. USA) werden, sofern kein Angemessenheitsbeschluss vorliegt, die Standardvertragsklauseln der EU-Kommission als Garantie für ein angemessenes Datenschutzniveau genutzt.
EU-U.S. Data Privacy Framework	Die US-Muttergesellschaften bzw. US-Anbieter der oben genannten Dienste (u. a. Google, Microsoft, Stripe, PostHog, Slack, Twilio, ElevenLabs) sind unter dem DPF zertifiziert, was ein angemessenes Schutzniveau für die Datenübermittlung in die USA bestätigt.