Auftragsverarbeitungsvertrag (AVV)

Stand: Juni 2026 · Version 1.0

Parteien

Zwischen **Janeway.io UG (haftungsbeschränkt)**, August-Bebel-Straße 16, 16816 Neuruppin, eingetragen im Handelsregister des Amtsgericht Neuruppin unter HRB 15191 NP, vertreten durch den Geschäftsführer Lukas Pritzkow (nachfolgend „**Auftragnehmer**")

und

[Firmenname des Auftraggebers], [Straße, Hausnummer], [PLZ Ort], [Land], eingetragen im Handelsregister des [Amtsgericht], HRB [Nummer], vertreten durch [Name, Funktion] (nachfolgend „**Auftraggeber**")

— gemeinsam die „**Parteien**" —

Dieser Auftragsverarbeitungsvertrag (nachfolgend „**AVV**") regelt die Verarbeitung personenbezogener Daten durch Janeway.io UG (haftungsbeschränkt) (nachfolgend „**Auftragsverarbeiter**") im Auftrag des Auftraggebers (nachfolgend „**Verantwortlicher**") gemäß Art. 28 DSGVO.

Präambel und Rahmenangaben

Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Bereitstellung einer cloudbasierten KI-Software-Suite (Janeway Suite) einschließlich KI-Assistenz, Workflow-Automatisierung, Kontakt- und Aufgabenverwaltung, Kalender, Notizen, Übersetzungsdienste sowie ergänzender Module (nachfolgend „**Hauptvertrag**" bzw. „**Dienste**").

Im Rahmen dieser Leistungserbringung verarbeitet der Auftragsverarbeiter personenbezogene Daten für und im Auftrag des Verantwortlichen. Die nachfolgenden Regelungen konkretisieren die datenschutzrechtlichen Pflichten beider Parteien.

1. Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die technische Bereitstellung und der Betrieb der Janeway Suite für den Verantwortlichen, einschließlich der Speicherung, Verarbeitung, Übermittlung und Nutzung der vom Verantwortlichen oder seinen Nutzern eingegebenen Daten zur Erbringung der vertraglich vereinbarten Funktionen.

2. Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des Hauptvertrags (Abonnement- bzw. Nutzungsvertrag). Nach Beendigung des Hauptvertrags endet die Verarbeitung gemäß § 7 dieses AVV (Löschung und Rückgabe).

3. Art und Zweck der Verarbeitung

Die Verarbeitung dient ausschließlich der Erbringung der im Hauptvertrag vereinbarten Dienste. Art der Verarbeitung: Erhebung, Speicherung, Verarbeitung (inkl. KI-gestützter Analyse), Übermittlung, Bereitstellung, Abruf, Löschung personenbezogener Daten über die Janeway Suite-Infrastruktur.

4. Art der personenbezogenen Daten

Je nach genutzten Modulen können folgende Datenkategorien betroffen sein:

- **Stammdaten:** Name, E-Mail-Adresse, Telefonnummer, Anschrift, Organisationszugehörigkeit

- **Kommunikationsinhalte:** Chat-Verläufe, KI-Antworten, Notizinhalte, Aufgabenbeschreibungen, Kalendereinträge
- **Verkehrsdaten:** Log-Daten, Nutzungsstatistiken, Zeitstempel, IP-Adressen
- **Audio-/Sprachdaten:** Sprachaufnahmen (Voice-Funktion), Transkripte (nur bei Nutzung KI-Telefonie)
- **Transaktionsdaten:** Abrechnungsdaten, Credit-Verbrauch (soweit durch Verantwortlichen eingegeben)
- **Inhaltsdaten:** Dokumente, Dateien, Medien, Exposé-Daten (bei Nutzung Immobilien-Modul)

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der bestimmungsgemäßen Verarbeitung. Sollte der Verantwortliche solche Daten gleichwohl eingeben, liegt die datenschutzrechtliche Verantwortung hierfür beim Verantwortlichen; der Verantwortliche hat sicherzustellen, dass eine entsprechende Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vorliegt.

5. Kategorien betroffener Personen

- Mitarbeiter, Beschäftigte und Auftragnehmer des Verantwortlichen
- Kunden, Interessenten und Geschäftspartner des Verantwortlichen
- Kontaktpersonen Dritter (soweit vom Verantwortlichen in die Dienste eingegeben)

6. Rechte und Pflichten des Verantwortlichen

Der Verantwortliche bleibt im Sinne des Datenschutzrechts allein verantwortlich für die Rechtmäßigkeit der Datenverarbeitung. Er ist insbesondere berechtigt und verpflichtet:

- dem Auftragsverarbeiter Weisungen zur Verarbeitung zu erteilen (§ 1 dieses AVV);
- die Einhaltung dieses AVV zu kontrollieren (§ 8 dieses AVV);
- Betroffenenrechte sicherzustellen und den Auftragsverarbeiter dabei in Anspruch zu nehmen (§ 5 dieses AVV);
- den Auftragsverarbeiter unverzüglich zu informieren, wenn er Weisungsverstöße feststellt.

§ 1 Weisungsgebundenheit (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder des Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

(2) Weisungen erteilt der Verantwortliche in Textform (E-Mail genügt). Der Auftragsverarbeiter führt ein **Weisungsregister**, in dem Datum, Inhalt und ausführende Person jeder Weisung dokumentiert werden. Das Weisungsregister ist dem Verantwortlichen auf Verlangen vorzulegen.

(3) Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, bedürfen einer gesonderten Vereinbarung einschließlich etwaiger Vergütungsregelungen.

(4) Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, hat er den Verantwortlichen unverzüglich zu informieren. Er ist berechtigt, die Ausführung bis zur Klärung auszusetzen.

(5) Weisungen im Sinne dieses AVV umfassen auch Weisungen zur Datenübermittlung in Drittländer. Ohne ausdrückliche Weisung des Verantwortlichen erfolgt keine Übermittlung in Drittländer, es sei denn, dies ist nach diesem AVV (Anlage 3) ausdrücklich vorgesehen.

§ 2 Vertraulichkeit der Verarbeitungsbefugten (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

(1) Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung befugten Personen die Vertraulichkeit der Daten gewährleisten. Die zur Verarbeitung befugten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht.

(2) Die Vertraulichkeitsverpflichtungen werden in Form von Vertraulichkeitserklärungen dokumentiert. Diese sind für die Dauer des AVV und darüber hinaus aufzubewahren und dem Verantwortlichen auf Verlangen nachweisbar vorzulegen.

(3) Nur solche Personen erhalten Zugang zu den Daten des Verantwortlichen, die diesen für die Erfüllung des Hauptvertrags benötigen (Need-to-know-Prinzip).

§ 3 Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Der Auftragsverarbeiter trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die TOM sind in **Anlage 2** dieses AVV vollständig beschrieben.

(2) Der Auftragsverarbeiter ist berechtigt, die TOM weiterzuentwickeln, soweit das Schutzniveau nicht unterschritten wird. Über wesentliche Änderungen an den TOM informiert er den Verantwortlichen vorab in Textform.

(3) Die TOM sind Mindeststandard. Der Verantwortliche kann weitergehende Maßnahmen durch Weisung gemäß § 1 vorgeben; etwaige Mehrkosten trägt der Verantwortliche.

§ 4 Sub-Auftragsverarbeiter (Art. 28 Abs. 2 und Abs. 4 DSGVO)

(1) **Allgemeine Genehmigung:** Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Beauftragung von Sub-Auftragsverarbeitern gemäß der in **Anlage 3** geführten Liste.

(2) **Informationspflicht vor Änderungen:** Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen — Hinzufügung oder Ersetzung von Sub-Auftragsverarbeitern — mindestens **30 Tage** vor dem geplanten Einsatz in Textform.

(3) **Einspruchsrecht:** Der Verantwortliche kann gegen einen neuen oder geänderten Sub-Auftragsverarbeiter aus berechtigtem Grund schriftlich Einspruch erheben. Berechtigte Gründe sind insbesondere: unzureichende TOM, Drittlandtransfer ohne geeigneten Schutzmechanismus, Konkurrenzsituation zum Verantwortlichen. Der Einspruch ist innerhalb von **14 Tagen ab Zugang** der Mitteilung nach Abs. 2 schriftlich zu erklären.

(3a) **Suspensiveffekt:** Erhebt der Verantwortliche fristgerecht Einspruch, setzt der Auftragsverarbeiter den betroffenen Sub-Auftragsverarbeiter bis zur einvernehmlichen Klärung **nicht** für die Verarbeitung personenbezogener Daten des Verantwortlichen ein. Kommt keine einvernehmliche Lösung zustande, ist der Verantwortliche berechtigt, diesen AVV und den Hauptvertrag außerordentlich zu kündigen.

(4) **Back-to-Back:** Der Auftragsverarbeiter legt jedem Sub-Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die ihm nach diesem AVV gegenüber dem Verantwortlichen obliegen (Art. 28 Abs. 4 DSGVO). Die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen bleibt davon unberührt.

(5) **Drittlandtransfers durch Sub-Auftragsverarbeiter:** Soweit Sub-Auftragsverarbeiter ihren Sitz in Drittländern haben oder dort Verarbeitungen vornehmen, werden die in Anlage 3 je Empfänger angegebenen geeigneten Garantien vorgehalten. Maßgeblich ist der jeweils einschlägige Mechanismus: Angemessenheitsbeschluss nach Art. 45 DSGVO (EU-U.S. Data Privacy Framework) für DPF-zertifizierte Anbieter (Stripe Inc., Google LLC, Microsoft Azure, Twilio Inc., Vonage, Perplexity AI Inc., CartoDB Inc./CARTO), ergänzend EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO; für **OpenAI (OpenAI, L.L.C.) und Anthropic PBC** (keine gesicherte DPF-Zertifizierung):

EU-Standardvertragsklauseln (Art. 46 DSGVO) nebst Transfer-Impact-Assessment sowie — bei aktivem Apex-Modus — ausdrückliche Einwilligung nach Art. 49 Abs. 1 lit. a DSGVO; Mistral AI (Frankreich): kein Drittlandtransfer. Die konkrete Zuordnung je Sub-Auftragsverarbeiter ergibt sich aus Anlage 3.

§ 5 Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 Satz 2 lit. e DSGVO)

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen dabei, seinen Pflichten gegenüber betroffenen Personen nachzukommen, insbesondere bei:

- Auskunft (Art. 15 DSGVO), Datenportabilität (Art. 20 DSGVO): Bereitstellung von Datenexporten auf Anfrage
- Berichtigung (Art. 16 DSGVO): Korrektur oder Aktualisierung von Datensätzen
- Löschung (Art. 17 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO): technische Umsetzung auf Weisung
- Widerspruch (Art. 21 DSGVO): Markierung betroffener Datensätze

(2) Eingehende Anfragen betroffener Personen, die sich an den Auftragsverarbeiter richten, leitet dieser unverzüglich, spätestens innerhalb von **72 Stunden**, an den Verantwortlichen weiter. Diese kurze Weiterleitungsfrist stellt sicher, dass dem Verantwortlichen die volle gesetzliche Frist zur Beantwortung gegenüber der betroffenen Person (ein Monat ab Eingang, Art. 12 Abs. 3 DSGVO) zur Verfügung steht. Der Auftragsverarbeiter beantwortet Betroffenenanfragen nicht im eigenen Namen, es sei denn, der Verantwortliche weist ihn ausdrücklich an.

(3) Die Unterstützungsleistungen nach Abs. 1 sind — soweit sie über den vertraglich vereinbarten Leistungsumfang hinausgehen — vergütungspflichtig. Die Vergütung richtet sich nach dem im jeweiligen Leistungsschein oder Angebot vereinbarten Stundensatz.

§ 6 Unterstützung bei Sicherheit und behördlichen Pflichten (Art. 28 Abs. 3 Satz 2 lit. f DSGVO)

(1) **Sicherheit (Art. 32 DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 DSGVO, insbesondere durch Bereitstellung der in Anlage 2 dokumentierten TOM-Nachweise.

(2) **Meldepflicht Datenpanne (Art. 33 DSGVO):** Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, in der Regel **innerhalb von 48 Stunden** nach Bekanntwerden. Die Meldung erfolgt per E-Mail an die vom Verantwortlichen benannte Kontaktstelle und enthält mindestens:

- eine Beschreibung der Art der Verletzung,
- die Kategorien und die ungefähre Anzahl der betroffenen Personen und Datensätze,
- die wahrscheinlichen Folgen und
- die ergriffenen oder vorgeschlagenen Maßnahmen.

Der Auftragsverarbeiter kann zunächst eine vorläufige Meldung mit den verfügbaren Informationen übermitteln und diese schrittweise ergänzen. Die gegenüber der gesetzlichen Frist verkürzte Meldefrist des Auftragsverarbeiters gewährleistet, dass dem Verantwortlichen ausreichend Zeit zur Erfüllung seiner 72-Stunden-Meldefrist (Art. 33 Abs. 1 DSGVO) gegenüber der Aufsichtsbehörde bleibt.

(3) **Benachrichtigung Betroffener (Art. 34 DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Weisung bei der Benachrichtigung betroffener Personen.

(4) **Datenschutz-Folgenabschätzung (Art. 35 DSGVO):** Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle erforderlichen Informationen für die Durchführung einer DSFA bereit.

(5) **Vorabkonsultation (Art. 36 DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage bei der Vorabkonsultation der Aufsichtsbehörde.

(6) Unterstützungsleistungen nach Abs. 3–5, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind vergütungspflichtig. Die Vergütung richtet sich nach dem im jeweiligen Leistungsschein oder Angebot vereinbarten Stundensatz.

§ 7 Löschung und Rückgabe nach Vertragsende (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

(1) **Wahlrecht des Verantwortlichen:** Nach Beendigung des Hauptvertrags — gleich aus welchem Grund — hat der Verantwortliche das Wahlrecht, vom Auftragsverarbeiter zu verlangen:

a) **Rückgabe** aller personenbezogenen Daten in einem maschinenlesbaren Format (CSV, JSON oder XML nach Wahl des Verantwortlichen), verschlüsselt übertragen, oder
b) **Löschung** aller personenbezogenen Daten (einschließlich etwaiger Kopien), oder
c) eine **Kombination** aus Rückgabe bestimmter Datenkategorien und Löschung der übrigen.

(2) **Frist und Default-Regel:** Der Verantwortliche teilt seine Wahl nach Abs. 1 dem Auftragsverarbeiter spätestens **30 Tage** nach Beendigung des Hauptvertrags mit. Der Auftragsverarbeiter führt Rückgabe oder Löschung innerhalb von **30 Tagen** nach Eingang der Weisung durch. Teilt der Verantwortliche seine Wahl nicht innerhalb der genannten 30 Tage mit, weist der Auftragsverarbeiter ihn vor Ablauf dieser Frist mindestens einmal in Textform auf die ausstehende Wahl und die Folge der unterbleibenden Mitteilung hin. Erfolgt auch danach keine Wahl, **löscht** der Auftragsverarbeiter nach Ablauf der 30-Tage-Frist datenschutzkonform alle personenbezogenen Daten (Default-Löschung); eine etwaige Rückgabe ist dann nicht mehr möglich. Gesetzliche Aufbewahrungspflichten nach Abs. 6 bleiben unberührt.

(3) **Format und Übertragung:** Die Datenrückgabe erfolgt in einem offenen, maschinenlesbaren Format (CSV, JSON oder XML). Der Transport erfolgt verschlüsselt (HTTPS/SFTP). Details zu Format und Übertragungsweg regelt **Anlage 4** (Löschkonzept).

(4) **Backups:** Sicherungskopien (Backups) werden spätestens **90 Tage** nach dem Datum der Rückgabe oder Löschung endgültig und unwiederbringlich gelöscht.

(5) **Löschstandard:** Löschvorgänge erfolgen nach dem Standard DIN 66399 / NIST SP 800-88 (Kategorie nach Datenträgertyp). Dies schließt die Löschung von Daten bei Sub-Auftragsverarbeitern gemäß § 4 Abs. 4 ein.

(6) **Gesetzliche Aufbewahrungspflichten:** Daten, die gesetzlichen Aufbewahrungspflichten unterliegen (insbesondere §§ 257, 261 HGB, § 147 AO), werden bis zum Ablauf der jeweiligen gesetzlichen Frist gesperrt, d.h. von der aktiven Verarbeitung ausgeschlossen und ausschließlich zur Erfüllung der Aufbewahrungspflicht vorgehalten. Nach Ablauf der Frist werden sie unverzüglich gelöscht. Der Verantwortliche ist hiervon vorab in Kenntnis zu setzen.

(7) **Löschprotokoll:** Der Auftragsverarbeiter erstellt nach Abschluss der Löschung ein schriftliches **Löschprotokoll**, das Datum, angewandte Methode und verantwortliche Person ausweist, und übermittelt dieses an den Verantwortlichen. Auf Verlangen legt der Auftragsverarbeiter entsprechende Löschnachweise der Sub-Auftragsverarbeiter vor.

§ 8 Audit- und Kontrollrechte (Art. 28 Abs. 3 Satz 2 lit. h DSGVO)

(1) **Informationsrecht:** Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieses AVV zur Verfügung, insbesondere Dokumentationen, Weisungsregister, TOM-Nachweise und Vertraulichkeitserklärungen.

(2) **Kontrollrechte:** Der Verantwortliche oder ein von ihm beauftragter Drittprüfer (z.B. Datenschutzbeauftragter, Wirtschaftsprüfer, zertifizierter Datenschutzauditor) ist berechtigt, die Einhaltung dieses AVV durch Vor-Ort-Prüfungen, Dokumentensichtungen oder Fragebogen zu kontrollieren.

(3) **Ankündigung und Frequenz:** Audits sind dem Auftragsverarbeiter mindestens **4 Wochen** im Voraus in Textform anzukündigen und auf das erforderliche Maß zu beschränken. Pro Kalenderjahr ist ein Audit-Recht ohne gesonderte Begründung vorgesehen; weitere Audits bedürfen eines besonderen Anlasses (z.B. sicherheitsrelevantes Ereignis).

(4) **Kostenträger:** Die Kosten der Vorbereitung und Begleitung durch den Auftragsverarbeiter für ein reguläres Jahres-Audit sind im Auftragsverarbeitungsverhältnis eingeschlossen; bei Anlassaudits und bei Beauftragung externer Prüfer trägt der Verantwortliche die entstehenden Mehrkosten des Auftragsverarbeiters nach Aufwand.

(5) **Nachweisersatz:** Statt Vor-Ort-Audits kann der Auftragsverarbeiter anerkannte Zertifizierungen oder Testate (z.B. ISO 27001, SOC 2, BSI C5) als gleichwertigen Nachweis vorlegen. Das Recht auf eigene Vor-Ort-Kontrolle nach Abs. 2 bleibt davon unberührt.

§ 9 Haftung

(1) Jede Partei haftet gegenüber der jeweils anderen Partei für Schäden, die durch Verstöße gegen diesen AVV entstehen, nach den allgemeinen gesetzlichen Bestimmungen, soweit nachfolgend nicht abweichend geregelt.

(2) Die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen für einfache Fahrlässigkeit ist — soweit gesetzlich zulässig — auf den im Hauptvertrag für das jeweilige Vertragsjahr gezahlten Vergütungsbetrag begrenzt, mindestens jedoch auf 5.000 EUR je Schadensfall. Diese Begrenzung gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, für Schäden aus der Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), für Vorsatz oder grobe Fahrlässigkeit sowie bei Ansprüchen nach dem Produkthaftungsgesetz und aus zugesicherten Eigenschaften.

(3) Im Außenverhältnis zu Betroffenen nach Art. 82 DSGVO haftet jede Partei nur für den Schaden, den sie zu verantworten hat. Das Regressverhältnis der Parteien untereinander richtet sich nach Art. 82 Abs. 4 und 5 DSGVO: Der Auftragsverarbeiter kann sich gegenüber dem Verantwortlichen auf Entlastung berufen, soweit er nachweist, dass ihn kein Verschulden trifft.

§ 10 Schlussbestimmungen

(1) **Vorrang:** Dieser AVV geht im Falle von Widersprüchen mit dem Hauptvertrag in Bezug auf datenschutzrechtliche Regelungen vor.

(2) **Schriftform:** Änderungen und Ergänzungen dieses AVV bedürfen der Textform.

(3) **Anwendbares Recht:** Es gilt deutsches Recht. Gerichtsstand ist Neuruppin, soweit gesetzlich zulässig.

(4) **Salvatorische Klausel:** Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit des übrigen AVV unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

Anlage 1: Beschreibung der Verarbeitung

Diese Anlage konkretisiert die Rahmenangaben nach Art. 28 Abs. 3 Satz 2 DSGVO und ist Bestandteil des AVV.

Merkmal	Beschreibung

Gegenstand	Bereitstellung und Betrieb der Janeway Suite (cloudbasierte KI-Software)
Dauer	Laufzeit des Hauptvertrags + 30-Tage-Nachlauffrist für Rückgabe/Löschung
Art der Verarbeitung	Erhebung, Speicherung, Verarbeitung (inkl. KI-Analyse), Bereitstellung, Löschung
Zweck	Erbringung der vertraglich vereinbarten SaaS-Dienste
Datenkategorien	Stammdaten, Kommunikationsinhalte, Verkehrs-/Logdaten, Audio-/Sprachdaten (opt.), Transaktionsdaten, Inhaltsdaten
Betroffene Personen	Mitarbeiter/Auftragnehmer des Verantwortlichen; Kunden/Geschäftspartner des Verantwortlichen; Kontaktpersonen Dritter
Drittlandtransfers	Für Zahlungsabwicklung (Stripe, USA), Telefonie/SIP (Vonage, Twilio, USA) und den optionalen Apex-Modus (USA). Grundlage je Empfänger: Angemessenheitsbeschluss (Art. 45 DSGVO / EU-US Data Privacy Framework), EU-Standardvertragsklauseln (Art. 46 DSGVO) oder — Apex-Modus ohne Angemessenheitsbeschluss — ausdrückliche Einwilligung (Art. 49 Abs. 1 lit. a DSGVO). Einzelheiten in Anlage 3

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Diese Anlage ergänzt § 3 dieses AVV und dokumentiert die nach Art. 32 DSGVO getroffenen Maßnahmen.

Wir treffen geeignete technische und organisatorische Maßnahmen (Art. 32 DSGVO), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

- **Transportverschlüsselung:** Alle Datenübertragungen sind durch TLS/SSL (HTTPS) verschlüsselt.
- **Speicherverschlüsselung:** Gespeicherte Daten werden mit AES-256 verschlüsselt (Verschlüsselung at rest).
- **Zugriffskontrollen:** Strikte rollenbasierte Zugriffsberechtigungen begrenzen den Datenzugriff auf das jeweils erforderliche Minimum.
- **Multi-Faktor-Authentifizierung (MFA):** Alle Administrationszugänge sind durch MFA gesichert.
- **Sicherheitsaudits und Penetrationstests:** Wir führen regelmäßige Sicherheitsüberprüfungen und Penetrationstests durch.
- **Hosting in EU/DE-Rechenzentren:** Das Kern-Hosting erfolgt bei der Hetzner Online GmbH in Deutschland.
- **Datensparsamkeit:** Wir verarbeiten personenbezogene Daten nur im erforderlichen Umfang und löschen diese nach definierten Fristen (siehe Abschnitt Speicherdauer und Löschung).

Ergänzende AVV-spezifische Maßnahmen

- **Pseudonymisierung/Datentrennung (Trennungskontrolle):** Kundendaten werden mandantenfähig und logisch getrennt verarbeitet; kein Zugriff zwischen verschiedenen Kundenmandanten.

- **Backup und Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):** Tägliche verschlüsselte Datensicherungen; RPO d 24 Stunden; RTO d 8 Stunden (kritische Verarbeitungen); mindestens halbjährliche Restore-Tests.
- **Belastbarkeit und Verfügbarkeit:** DDoS-Schutz auf Infrastrukturebene; Failover-Mechanismen; angestrebte Verfügbarkeit 99,5 % im Monatsmittel, gemessen außerhalb geplanter Wartungsfenster.
- **Weitergabekontrolle (Logging):** Zugriffe auf personenbezogene Daten werden protokolliert und für 90 Tage aufbewahrt.
- **Regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d DSGVO):** Jährliche externe Penetrationstests; monatliche automatisierte Vulnerability-Scans; Ergebnisse werden dokumentiert und Maßnahmen verfolgt.

Anlage 3: Genehmigte Sub-Auftragsverarbeiter

Diese Anlage ergänzt § 4 dieses AVV. Änderungen werden dem Verantwortlichen gemäß § 4 Abs. 2 mit einer Frist von 30 Tagen vorab mitgeteilt.

Zur Erbringung unserer Dienste setzen wir folgende Auftragsverarbeiter ein, mit denen Verträge zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO abgeschlossen wurden. Bei Empfängern in Drittländern ist der konkrete Übermittlungsmechanismus angegeben (Art. 45 Angemessenheitsbeschluss / EU-US Data Privacy Framework, Art. 46 Standardvertragsklauseln oder Art. 49 Abs. 1 lit. a ausdrückliche Einwilligung).

Anbieter	Sitz / Region	Zweck	Drittland-Mechanismus
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Deutschland	Kern-Hosting Server-Infrastruktur (Website, Apps, KI-Dienste)	kein Drittland
Microsoft Azure	EU / West Europe	Technische Schnittstelle Speech-to-Text, LLM, Text-to-Speech (DSGVO-konformer Modus)	EU; keine Nutzung zum Training globaler Modelle
Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland	Irland (EU)	Zahlungsabwicklung kostenpflichtiger Abonnements	bei Übermittlung an Stripe Inc. (USA): Angemessenheitsbeschluss (Art. 45 DSGVO) auf Grundlage des EU-US Data Privacy Framework, ergänzend EU-Standardvertragsklauseln (Art. 46 DSGVO)

Vonage (USA) / Twilio Inc. (USA)	USA	Telefonie/Sprachverbindung (SIP-Trunk): Vonage als primärer SIP-Provider; Twilio Inc. u. a. SMS-Versand. Verarbeitet werden Rufnummern, Verbindungs- und ggf. Gesprächsinhaltsdaten. Der Echtzeit-Medientransport läuft über selbst betriebenes LiveKit.	Art. 45 DSGVO (EU-U.S. Data Privacy Framework, beide Anbieter DPF-zertifiziert), ergänzend Standardvertragsklauseln (Art. 46 DSGVO)
Google LLC / Perplexity AI, Inc. / CartoDB Inc. (CARTO)	überwiegend USA	**Ausschließlich im optionalen Apex-Modus** (s.u.) bzw. Kartendienste	Angemessenheitsbeschluss (Art. 45 DSGVO / EU-US Data Privacy Framework); ergänzend Standardvertragsklauseln (Art. 46 DSGVO)
OpenAI (OpenAI, L.L.C.) / Anthropic PBC	USA	**Ausschließlich im optionalen Apex-Modus** (s.u.)	keine (gesicherte) DPF-Zertifizierung; Standardvertragsklauseln (Art. 46 DSGVO) nebst Transfer-Impact-Assessment; bei aktivem Apex-Modus zusätzlich ausdrückliche Einwilligung (Art. 49 Abs. 1 lit. a DSGVO)
Mistral AI	Frankreich (EU)	**Ausschließlich im optionalen Apex-Modus** (s.u.)	kein Drittlandtransfer (EU)
Eigene SMTP-Infrastruktur	Deutschland	E-Mail-Versand (z.B. Kontaktformular-Bestätigungen)	kein Drittland

Die in der Tabelle angegebenen Übermittlungsmechanismen sind anbieterbezogen festgelegt; die DPF-Zertifizierung der in den USA ansässigen Anbieter (Stripe, Google, Microsoft/Azure, Twilio, Vonage, Perplexity, CARTO) wird mindestens jährlich überprüft. Für OpenAI und Anthropic besteht keine gesicherte DPF-Zertifizierung; deren Übermittlungen stützen sich auf Standardvertragsklauseln (Art. 46 DSGVO) nebst Transfer-Impact-Assessment und im Apex-Modus zusätzlich auf die ausdrückliche Einwilligung (Art. 49 Abs. 1 lit. a DSGVO). Eingegebene Inhalte werden nicht zum Training von KI-Modellen verwendet.

Stand der Sub-Prozessoren-Liste: Juni 2026. Die Liste wird bei Änderungen aktualisiert; das jeweilige Versionsdatum ist hier ausgewiesen.

KI-Verarbeitungsmodi

Sentinel & Cortex (DSGVO-konformer Modus): Diese KI-Dienste nutzen ausschließlich Modelle, die in Rechenzentren innerhalb der EU/des EWR gehostet werden. Eine Übermittlung von Inhalten in Drittländer findet dabei nicht statt.

Apex (optionaler Modus): Apex ist ein optionaler Modus, der nur nach Ihrer aktiven Auswahl genutzt wird und außerhalb des EU-Standard- und Datenresidenz-Betriebs liegt. Bei aktiver Auswahl werden Anfrageinhalte an KI-Anbieter mit

Sitz in Drittländern (u. a. USA) übermittelt, etwa OpenAI, Anthropic, Google und Perplexity. Rechtsgrundlage der Übermittlung ist Ihre **ausdrückliche Einwilligung nach Art. 49 Abs. 1 lit. a DSGVO** nach Hinweis auf das ggf. fehlende EU-Datenschutzniveau bei Anbietern ohne Angemessenheitsbeschluss. Soweit ein Anbieter über eine gültige Zertifizierung nach dem EU-US Data Privacy Framework verfügt, erfolgt die Übermittlung auf Grundlage des entsprechenden Angemessenheitsbeschlusses (Art. 45 DSGVO). Wir empfehlen, im Apex-Modus keine besonders sensiblen personenbezogenen Daten zu verarbeiten.

Der einsetzbare KI-Modell-Katalog ist konfigurierbar; ein Modell ist nur aktiv, wenn die hierfür erforderlichen Zugangsdaten hinterlegt sind. Standardmäßig vorgesehene Anbieter: **OpenAI, Anthropic, Google, Mistral (EU), Microsoft Azure und Perplexity**. Für DSGVO- und behördliche Kontexte werden ausschließlich Anbieter mit Angemessenheitsbeschluss (DPF) oder Standardvertragsklauseln eingesetzt. Anbieter mit Datenverarbeitung in Drittländern **ohne** Angemessenheitsbeschluss und ohne tragfähige Garantien — **insbesondere Anbieter mit Verarbeitung in der Volksrepublik China (z. B. DeepSeek)** — sind hierfür **nicht vorgesehen** und werden produktiv nicht freigeschaltet.

Die konkreten Drittland-Schutzmechanismen je Sub-Auftragsverarbeiter ergeben sich aus der vorstehenden Sub-Prozessoren-Übersicht: Angemessenheitsbeschluss (Art. 45 DSGVO / EU-U.S. Data Privacy Framework) für die DPF-zertifizierten Anbieter Stripe, Google, Microsoft/Azure, Twilio, Vonage, Perplexity und CartoDB (CARTO), ergänzend EU-Standardvertragsklauseln (Art. 46 DSGVO); für **OpenAI (OpenAI, L.L.C.) und Anthropic PBC** EU-Standardvertragsklauseln (Art. 46 DSGVO) nebst Transfer-Impact-Assessment sowie — bei aktivem Apex-Modus — ausdrückliche Einwilligung (Art. 49 Abs. 1 lit. a DSGVO); Mistral AI (Frankreich) und Microsoft Azure (EU West Europe): kein Drittlandtransfer. Die DPF-Zertifizierung wird vom Auftragsverarbeiter mindestens jährlich überprüft.

Anlage 4: Löschkonzept

Diese Anlage ergänzt § 7 dieses AVV und beschreibt das Vorgehen bei Datenrückgabe und -löschung nach Vertragsende.

Wahlrecht und Frist

Der Verantwortliche teilt seine Wahl (Rückgabe, Löschung oder Kombination) innerhalb von 30 Tagen nach Vertragsende schriftlich mit (§ 7 Abs. 2). Vor Ablauf dieser Frist erinnert der Auftragsverarbeiter den Verantwortlichen mindestens einmal in Textform an die ausstehende Wahl. Ohne fristgerechte Mitteilung löscht der Auftragsverarbeiter nach Ablauf der 30-Tage-Frist datenschutzkonform alle personenbezogenen Daten endgültig (Default-Löschung). Gesetzliche Aufbewahrungspflichten bleiben unberührt.

Datenrückgabe

Merkmal	Details
Formate	CSV, JSON, XML (Wahl des Verantwortlichen)
Umfang	Alle verarbeiteten personenbezogenen Daten, sofern technisch exportierbar und nicht gesetzlich gesperrt
Transport	Verschlüsselt via HTTPS-Download oder SFTP; Zugangslink mit Ablaufdatum
Frist	30 Tage nach schriftlicher Weisung

Löschung

Merkmal	Details
Standard	DIN 66399 / NIST SP 800-88 (Löschklasse nach Datenträgertyp)
Backups	Werden spätestens 90 Tage nach Produktivlöschung endgültig gelöscht
Sub-Auftragsverarbeiter	Löschanweisung an alle in Anlage 3 genannten Sub-AV; Löschnachweise auf Verlangen vorlegen
Sperrung gesetzlich aufbewahrungspflichtiger Daten	Daten nach §§ 257 HGB, 147 AO werden bis zum Fristablauf gesperrt, danach gelöscht

Löschprotokoll

Nach Abschluss erstellt der Auftragsverarbeiter ein Löschprotokoll mit Angabe von:

- Datum der Löschung/Rückgabe
- Angewandter Methode
- Verantwortliche Person (Name/Funktion)
- Bestätigung der Löschung bei Sub-AV (oder Verweis auf deren Nachweis)

Das Löschprotokoll wird dem Verantwortlichen innerhalb von 14 Tagen nach Abschluss übermittelt.