

Auftragsverarbeitungsvertrag (AVV) gemaess Art. 28 DSGVO

Stand: 30.04.2026, Version 1.1

§ 1 Gegenstand und Dauer

1.1 Dieser Auftragsverarbeitungsvertrag (AVV) konkretisiert die datenschutzrechtlichen Pflichten der Vertragsparteien gemäß Art. 28 DSGVO im Zusammenhang mit der Nutzung der von Tech4Humans bereitgestellten Dienste.

1.2 Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Tech4Humans) im Auftrag des Verantwortlichen (Kunde) im Rahmen des zwischen den Parteien bestehenden Hauptvertrages (AGB, Subscription Terms, individuelle Vereinbarungen).

1.3 Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages. Der AVV endet automatisch mit Beendigung des Hauptvertrages, sofern keine abweichende Regelung getroffen wurde.

1.4 Der Auftragsverarbeiter verarbeitet personenbezogene Daten soweit technisch möglich im Europäischen Wirtschaftsraum (EWR). Drittlandtransfers erfolgen nur unter den Voraussetzungen der Art. 44 ff. DSGVO (siehe §8 Unterauftragsverarbeitung).

§ 2 Art und Zweck der Verarbeitung

2.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen zum Zweck der:

- Bereitstellung und Betrieb des AE WebPack (AWP) – eingebettetes Chat-Widget, Kontaktformulare, KI-gestützte Kommunikation
- Verarbeitung und Speicherung von Kontaktanfragen über das AWP-Widget
- Versand von Bestätigungs-, Einwilligungs- und Statusmitteilungen per E-Mail und/oder WhatsApp im Namen des Verantwortlichen
- Bereitstellung und Betrieb digitaler Mitarbeiter (Artificial Employees / AE) einschließlich KI-gestützter Kommunikation
- Speicherung und Verwaltung von Nutzerprofilen, Einwilligungen und Kommunikationsverläufen
- Technische Analyse und Optimierung der bereitgestellten Dienste (Logging, Fehleranalyse, Performance-Monitoring)

2.2 Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen (siehe §5). Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

2.3 KI-gestützte Verarbeitung: Soweit KI-Systeme (Large Language Models, Speech-to-Text, Text-to-Speech) zum Einsatz kommen, werden personenbezogene Daten ausschließlich zur Echtzeit-Verarbeitung der jeweiligen Anfrage verwendet. Es findet kein Training von KI-Modellen mit personenbezogenen Daten des Verantwortlichen statt.

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1 Art der personenbezogenen Daten:

- Kontaktdaten: Vorname, Nachname, E-Mail-Adresse, Telefonnummer
- Unternehmensdaten: Firmenname, Position/Rolle
- Kommunikationsdaten: Chat-Verläufe, Nachrichten, Formulareinträge, Sprachaufnahmen
- Technische Daten: IP-Adresse, Browser-Typ, Gerätetyp, Zeitstempel, Referrer-URL
- Einwilligungsdaten: Consent-Status, Einwilligungszeitpunkt, Double-Opt-In-Status
- Nutzungsdaten: Seitenaufrufe, Interaktionen mit dem Widget, Session-Daten

3.2 Kategorien betroffener Personen:

- Besucher und Nutzer der Website des Verantwortlichen
- Interessenten und Kontaktpersonen, die über das AWP-Widget Anfragen stellen
- Bestandskunden des Verantwortlichen, die über das Widget kommunizieren
- Mitarbeiter des Verantwortlichen, soweit sie das System administrieren

3.3 Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO werden grundsätzlich nicht verarbeitet. Sollte der Verantwortliche solche Daten über das Widget erheben wollen, bedarf es einer gesonderten schriftlichen Vereinbarung und zusätzlicher technischer Schutzmaßnahmen.

§ 4 Pflichten und Rechte des Verantwortlichen

4.1 Der Verantwortliche ist für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er stellt sicher, dass:

- eine gültige Rechtsgrundlage für die Verarbeitung vorliegt (Art. 6 DSGVO)
- die betroffenen Personen ordnungsgemäß informiert werden (Art. 13, 14 DSGVO)
- erforderliche Einwilligungen eingeholt werden (Art. 7 DSGVO)
- die Verarbeitung in seiner Datenschutzerklärung vollständig dokumentiert ist
- der Einsatz des Auftragsverarbeiters in der Datenschutzerklärung benannt wird

4.2 Der Verantwortliche hat das Recht, Weisungen zur Verarbeitung zu erteilen und deren Einhaltung zu überprüfen.

4.3 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich über Fehler oder Unregelmäßigkeiten, die er bei der Prüfung der Verarbeitungsergebnisse feststellt.

4.4 Der Verantwortliche benennt dem Auftragsverarbeiter einen Ansprechpartner für datenschutzrelevante Fragen.

§ 5 Weisungsgebundenheit

5.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisungen des Verantwortlichen – einschließlich der in diesem AVV und im Hauptvertrag festgelegten Verarbeitungszwecke.

5.2 Weisungen können in Textform (E-Mail, Ticket-System, Chat) erteilt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

5.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

5.4 Die Konfiguration der AWP-Dienste durch den Verantwortlichen (z. B. Formularfelder, Datenschutz-URLs, Einwilligungstexte) gilt als dokumentierte Weisung im Sinne dieses Vertrages.

§ 6 Vertraulichkeit

6.1 Der Auftragsverarbeiter gewährleistet, dass alle Personen, die Zugang zu personenbezogenen Daten haben, zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

6.2 Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Vertragsverhältnisses fort.

6.3 Der Auftragsverarbeiter stellt sicher, dass nur diejenigen Mitarbeiter Zugang zu personenbezogenen Daten erhalten, die diesen zur Erfüllung ihrer Aufgaben zwingend benötigen (Need-to-know-Prinzip).

§ 7 Technische und organisatorische Maßnahmen (TOMs)

7.1 Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehören insbesondere:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO):

- Verschlüsselung der Datenübertragung (TLS 1.2+)
- Zugriffskontrolle durch rollenbasierte Berechtigungen
- Authentifizierung über sichere Verfahren (API-Keys, OAuth 2.0)
- Physische Zutrittskontrolle zum Rechenzentrum (IONOS, ISO 27001)

Integrität (Art. 32 Abs. 1 lit. b DSGVO):

- Eingabekontrolle durch Protokollierung von Schreibzugriffen
- Validierung eingehender Daten (Injection-Schutz, Input Sanitization)
- Regelmäßige Sicherheitsupdates und Patches

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO):

- Regelmäßige Datensicherungen (Backups)
- Redundante Serverinfrastruktur
- Monitoring und automatische Alarmierung bei Störungen

Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO):

- Regelmäßige Überprüfung der Wirksamkeit der TOMs
- Dokumentation und Versionierung der Sicherheitsmaßnahmen
- Incident-Response-Verfahren

7.2 Die detaillierten TOMs sind in Anlage 1 zu diesem AVV dokumentiert und werden bei wesentlichen Änderungen aktualisiert.

7.3 Der Auftragsverarbeiter überprüft die TOMs regelmäßig und passt sie dem aktuellen Stand der Technik an.

§ 8 Unterauftragsverarbeitung

8.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen (Art. 28 Abs. 2 DSGVO).

8.2 Zum Zeitpunkt des Abschlusses dieses AVV setzt der Auftragsverarbeiter folgende Unterauftragsverarbeiter ein:

- **IONOS SE** (Montabaur, Deutschland) – Hosting, Server-Infrastruktur, E-Mail-Versand. AVV abgeschlossen.
- **Microsoft Corporation** (EU-Rechenzentren) – Cloud-Dienste (Azure, Microsoft 365), E-Mail-/Kalender-Integration via OAuth. DPA in Online Service Terms enthalten.
- **Google LLC** (EU-Rechenzentren) – Cloud Data Processing, E-Mail-/Kalender-Integration via OAuth. Cloud Data Processing Amendment zertifiziert.
- **OpenAI, Inc.** (USA, EU DPF zertifiziert) – KI-Sprachverarbeitung (Large Language Models) für Chat-Funktionen. Digitaler DPA unterzeichnet. Keine Speicherung/Training mit Kundendaten (Zero Data Retention Policy).
- **Twilio Inc.** (USA, EU DPF zertifiziert) – SMS-/WhatsApp-Nachrichtenversand. DPA in Terms of Service enthalten.
- **Telnyx LLC** (USA, EU DPF zertifiziert / SCCs, Data Locality EU Germany) – Telefonie und SMS als Kommunikations-Transportdienst. DPA in Terms of Service enthalten. Telnyx AI Services werden nicht genutzt.

8.3 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 14 Tage vor der geplanten Hinzuziehung oder dem Wechsel eines Unterauftragsverarbeiters in Textform. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen widersprechen.

8.4 Bei begründetem Widerspruch ist der Auftragsverarbeiter berechtigt, den Hauptvertrag mit einer Frist von 30 Tagen zu kündigen, sofern eine Leistungserbringung ohne den betreffenden Unterauftragsverarbeiter nicht möglich oder zumutbar ist.

8.5 Der Auftragsverarbeiter stellt sicher, dass jedem Unterauftragsverarbeiter mindestens die gleichen Datenschutzpflichten auferlegt werden wie in diesem AVV vereinbart (Art. 28 Abs. 4 DSGVO).

8.6 Die aktuelle Liste der Unterauftragsverarbeiter ist jederzeit unter <https://tech4humans.de/avv> einsehbar.

§ 9 Unterstützung bei Betroffenenrechten

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Pflichten gegenüber betroffenen Personen (Art. 28 Abs. 3 lit. e DSGVO), insbesondere bei:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Mitteilungspflicht (Art. 19 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)

9.2 Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter.

9.3 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle für die Beantwortung von Betroffenenanfragen erforderlichen Informationen und Datenexporte innerhalb von 10 Werktagen zur Verfügung.

9.4 Löschanfragen betroffener Personen, die über die im Widget integrierten Widerrufsmechanismen eingehen, werden automatisiert verarbeitet und dem Verantwortlichen zur Kenntnis gebracht.

§ 10 Unterstützung bei Sicherheits- und Meldepflichten

10.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO), insbesondere bei:

- Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO)
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO)
- Benachrichtigung der betroffenen Personen (Art. 34 DSGVO)
- Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
- Vorherige Konsultation der Aufsichtsbehörde (Art. 36 DSGVO)

10.2 **Meldung von Datenschutzverletzungen:** Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden. Die Meldung enthält mindestens:

- Beschreibung der Art der Verletzung
- Betroffene Datenkategorien und ungefähre Anzahl betroffener Personen
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen und vorgeschlagenen Abhilfemaßnahmen

10.3 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Meldepflichten gegenüber der zuständigen Aufsichtsbehörde (Berliner Beauftragte für Datenschutz und Informationsfreiheit) und den betroffenen Personen.

§ 11 Löschung und Rückgabe

11.1 Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter sämtliche personenbezogene Daten, die im Auftrag des Verantwortlichen verarbeitet wurden, unwiderruflich und vollständig – es sei denn, der Verantwortliche wünscht eine Rückgabe oder gesetzliche Aufbewahrungspflichten stehen der Löschung entgegen (Art. 28 Abs. 3 lit. g DSGVO).

11.2 Der Verantwortliche kann vor der Löschung die Herausgabe aller Daten in einem gängigen, maschinenlesbaren Format (z. B. JSON, CSV) verlangen. Der Auftragsverarbeiter stellt die Daten innerhalb von 30 Tagen nach Vertragsende bereit.

11.3 Die Löschung erfolgt innerhalb von 60 Tagen nach Vertragsende, sofern keine Herausgabe verlangt wird. Der Auftragsverarbeiter bestätigt die vollständige Löschung auf Verlangen in Textform.

11.4 Gesetzliche Aufbewahrungspflichten (z. B. steuerrechtliche Pflichten, §§ 147 AO, 257 HGB) bleiben unberührt. In diesem Fall werden die Daten bis zum Ablauf der Aufbewahrungsfrist gesperrt und anschließend gelöscht.

§ 12 Kontroll- und Prüfrechte

12.1 Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV und der geltenden Datenschutzvorschriften durch den Auftragsverarbeiter zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO).

12.2 Überprüfungen können erfolgen durch:

- Schriftliche Auskunft des Auftragsverarbeiters
- Einsichtnahme in die TOMs und Datenschutzdokumentation
- Inspektionen vor Ort nach vorheriger Ankündigung (Frist: 14 Tage)
- Prüfung durch unabhängige Dritte (Auditoren, Sachverständige)

12.3 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung und duldet Überprüfungen.

12.4 Die Kosten einer Überprüfung trägt der Verantwortliche, es sei denn, die Überprüfung ergibt wesentliche Verstöße gegen diesen AVV.

§ 13 Haftung

13.1 Die Haftung der Parteien richtet sich nach den geltenden gesetzlichen Bestimmungen und den Regelungen des Hauptvertrages (AGB).

13.2 Der Auftragsverarbeiter haftet gegenüber betroffenen Personen gemäß Art. 82 DSGVO, soweit er seinen spezifisch auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder gegen rechtmäßige Weisungen des Verantwortlichen verstoßen hat.

13.3 Im Innenverhältnis haftet jede Partei für den Teil des Schadens, der durch ihren jeweiligen Verantwortungsbereich verursacht wurde. Der Auftragsverarbeiter haftet insbesondere für die ordnungsgemäße Umsetzung der technischen und organisatorischen Maßnahmen (§7) und die Einhaltung der Weisungen (§5).

§ 14 Laufzeit und Kündigung

14.1 Dieser AVV wird mit Unterzeichnung wirksam und gilt für die Dauer des Hauptvertrages.

14.2 Eine isolierte Kündigung dieses AVV ohne gleichzeitige Kündigung des Hauptvertrages ist nicht möglich, sofern der Hauptvertrag die Verarbeitung personenbezogener Daten erfordert.

14.3 Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragsverarbeiter wiederholt oder schwerwiegend gegen die Bestimmungen dieses AVV verstößt oder Weisungen des Verantwortlichen nachhaltig missachtet.

14.4 Nach Beendigung dieses AVV gelten die Regelungen zur Löschung und Rückgabe (§11) sowie zur Vertraulichkeit (§6) fort.

§ 15 Schlussbestimmungen

15.1 Änderungen und Ergänzungen dieses AVV bedürfen der Textform.

15.2 Sollten einzelne Bestimmungen dieses AVV unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Die unwirksame Bestimmung ist durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahe kommt.

15.3 Es gilt deutsches Recht. Gerichtsstand ist Berlin, sofern gesetzlich zulässig.

15.4 Der Verantwortliche bestätigt mit Nutzung der AWP-Dienste die Kenntnisnahme und Akzeptanz dieses AVV. Eine gesonderte Unterschrift ist bei elektronischem Vertragsschluss nicht erforderlich (Art. 28 Abs. 9 DSGVO).

15.5 Dieser AVV ist jederzeit in der aktuellen Version unter <https://tech4humans.de/avv> einsehbar.