

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

Version 1.1

AUFTRAGGEBER (VERANTWORTLICHER)

[Unternehmen]

[Straße und Hausnummer]

[PLZ] [Stadt], Deutschland

Vertreten durch: [Vorname] [Nachname] ([Funktion / Position])

E-Mail: [email@beispiel.de]

USt-ID: [USt-ID]

Lizenz-Domain: [domain.de]

AUFTRAGNEHMER (AUFTRAGSVERARBEITER)

Dan Pardella

Kreuzstraße 3

04103 Leipzig, Deutschland

E-Mail: hej@danpardella.de

USt-ID: [wird nachgetragen]

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand, Art und Zweck der Datenverarbeitung, die Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen ergeben sich aus **Anlage 1** zu diesem Vertrag.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des zugrundeliegenden Hauptvertrags über die Nutzung des AgentNice-Dienstes. Der Vertrag endet automatisch mit Beendigung des Hauptvertrags.

§ 2 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die vorliegenden Regelungen und Anlagen zu diesem Vertrag stellen solche dokumentierten Weisungen dar.

(2) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer ist in einem solchen Fall berechtigt, die Ausführung der betreffenden Weisung bis zur Klärung auszusetzen.

(3) Weitere Weisungen können vom Auftraggeber jederzeit erteilt werden. Sie sind schriftlich oder in elektronischer Form zu dokumentieren.

§ 3 Technische und organisatorische Maßnahmen (TOM)

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen sind in **Anlage 2** beschrieben. Der Auftragnehmer ist berechtigt, die Maßnahmen weiterzuentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer dokumentiert die Maßnahmen und stellt dem Auftraggeber auf Anfrage Nachweise zur Verfügung.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich für die in Anlage 1 bestimmten Zwecke.

(2) Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragnehmer unterstützt den Auftraggeber soweit möglich bei der Erfüllung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheit, Meldung von Datenschutzverletzungen, Folgenabschätzung, vorherige Konsultation).

(4) Der Auftragnehmer löscht oder gibt nach Wahl des Auftraggebers alle personenbezogenen Daten zurück, wenn dies nach Abschluss der Verarbeitung verlangt wird, sofern keine gesetzliche Verpflichtung zur Speicherung besteht.

§ 5 Unterauftragsverhältnisse

- (1) Der Einsatz von Unterauftragnehmern ist nur mit vorheriger schriftlicher Genehmigung des Auftraggebers zulässig. Der Auftraggeber erteilt hiermit eine allgemeine Genehmigung für den Einsatz der in **Anlage 3** aufgeführten Unterauftragnehmer.
- (2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung von Unterauftragnehmern und räumt dem Auftraggeber die Möglichkeit ein, gegen derartige Änderungen Einspruch zu erheben.
- (3) Werden Unterauftragnehmer eingesetzt, hat der Auftragnehmer diesen Unterauftragnehmern dieselben Datenschutzpflichten aufzuerlegen, die in diesem Vertrag vereinbart sind.

§ 6 Betroffenenrechte

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (Art. 15–22 DSGVO), soweit ihm dies nach Art und Umfang der Verarbeitung möglich ist.
- (2) Der Auftragnehmer leitet Anfragen von betroffenen Personen, die sich direkt an ihn richten, unverzüglich an den Auftraggeber weiter.

§ 7 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, die Einhaltung dieses Vertrags durch Inspektionen oder Audits zu überprüfen. Der Auftragnehmer gewährt dem Auftraggeber zu diesem Zweck Zugang zu den relevanten Informationen.
- (2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Prüfung durch eine Aufsichtsbehörde ansteht und Daten des Auftraggebers betroffen sein könnten.
- (3) Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen kann durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen erbracht werden.

§ 8 Datenpannen und Sicherheitsvorfälle

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit, spätestens innerhalb von 48 Stunden nach Bekanntwerden.
- (2) Die Mitteilung enthält mindestens folgende Angaben:

- Beschreibung der Art der Verletzung
- Kategorien und ungefähre Anzahl der betroffenen Personen
- Kategorien und ungefähre Anzahl der betroffenen Datensätze
- Wahrscheinliche Folgen der Verletzung
- Ergriffene oder vorgeschlagene Maßnahmen

(3) Meldepflichten nach Art. 33 DSGVO gegenüber der Aufsichtsbehörde liegen beim Auftraggeber als Verantwortlichem.

§ 9 Löschung und Rückgabe von Daten

(1) Nach Beendigung der Verarbeitung oder auf Verlangen des Auftraggebers löscht der Auftragnehmer alle personenbezogenen Daten oder gibt sie zurück, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht.

(2) Die Löschung ist zu dokumentieren und dem Auftraggeber auf Verlangen zu bestätigen.

§ 10 Vertraulichkeit

(1) Der Auftragnehmer verpflichtet sich, alle im Rahmen des Vertrags bekannt gewordenen vertraulichen Informationen des Auftraggebers auch nach Vertragsbeendigung vertraulich zu behandeln.

(2) Diese Pflicht gilt nicht für Informationen, die allgemein bekannt sind oder ohne Verschulden des Auftragnehmers bekannt werden.

§ 11 Haftung

(1) Für Schäden, die durch eine Verarbeitung entstehen, die den Weisungen des Auftraggebers entspricht, haftet der Auftraggeber. Der Auftragnehmer haftet nicht, wenn er nachweist, dass er für den schadenstiftenden Umstand nicht verantwortlich ist (Art. 82 Abs. 3 DSGVO).

(2) Im Übrigen gelten die haftungsrechtlichen Regelungen des Hauptvertrags.

§ 12 Laufzeit und Kündigung

(1) Dieser Vertrag tritt mit Unterzeichnung in Kraft und läuft auf unbestimmte Zeit, solange der Auftragnehmer personenbezogene Daten für den Auftraggeber verarbeitet.

(2) Er endet automatisch mit Beendigung des Hauptvertrags. Eine gesonderte Kündigung ist nicht erforderlich.

§ 13 Rechtswahl und Gerichtsstand

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(2) Gerichtsstand ist Leipzig, soweit gesetzlich zulässig.

§ 14 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

§ 15 Änderungen und Ergänzungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

(2) Der Auftragnehmer ist berechtigt, die Bedingungen dieses Vertrags bei gesetzlichen Änderungen oder Änderungen der Aufsichtsbehördenpraxis anzupassen. Der Auftraggeber wird über Änderungen informiert; widerspricht er nicht innerhalb von vier Wochen, gelten die Änderungen als genehmigt.

§ 16 Anlagen

Bestandteil dieses Vertrags sind folgende Anlagen:

- **Anlage 1:** Beschreibung der Verarbeitung (Zweck, Art der Daten, Kategorien betroffener Personen)
- **Anlage 2:** Technische und organisatorische Maßnahmen (TOM)
- **Anlage 3:** Unterauftragnehmer
- **Anlage 4:** Drittlandtransfer / Transfer Impact Assessment

§ 17 Vertragsschluss

Dieser Vertrag kommt durch elektronische Annahme durch den Auftraggeber im AgentNice-Kundenportal zustande. Das Datum und die IP-Adresse der Annahme werden protokolliert.

Akzeptiert am [Datum der Unterzeichnung]	IP-Adresse [IP-Adresse]
Lizenz-Domain [domain.de]	

MUSTER

Anlage 1: Beschreibung der Verarbeitung

Zweck der Verarbeitung

Betrieb eines KI-gestützten Chat-Agenten auf der Website des Auftraggebers zur automatisierten Beantwortung von Anfragen. Der Agent verarbeitet Gesprächsinhalte der Website-Besucher, um passende Antworten zu generieren.

Art der personenbezogenen Daten

- Gesprächsinhalte (Textnachrichten der Nutzer, inkl. möglicherweise enthaltener personenbezogener Daten wie Namen, Kontaktdaten, Sachverhalte)
- Technische Metadaten (IP-Adresse des Nutzers, Sitzungs-ID, Timestamp)
- Lizenzinhaberdaten (Name, E-Mail-Adresse, Unternehmensname, Domain des Lizenzinhabers)

Kategorien betroffener Personen

- Website-Besucher des Auftraggebers (Nutzer des Chat-Widgets)
- Vertragspartner des Auftraggebers (sofern Kontaktinformationen im Chat verwendet werden)
- Mitarbeiter und Ansprechpartner des Auftraggebers (Lizenzinhaberdaten)

Verarbeitungsort

Bundesrepublik Deutschland (Primärsystem: Hetzner-Rechenzentrum, Nürnberg). Für KI-Inferenz: USA (Anthropic, Inc.) — siehe Anlage 4 (Drittlandtransfer).

Speicherdauer

Chat-Inhalte (Gesprächsinhalte und Antworten)

Speicherdauer: Keine Speicherung. Der Verantwortliche hat aktuell keine Retention aktiviert.

Konfiguration: Der Verantwortliche kann die Speicherdauer im Mein-Konto-Bereich unter den hierfür vorgesehenen Stufen (0, 7, 14, 30, 60 oder 90 Tage) auswählen. Änderungen werden im Snapshot dieses Vertrags dokumentiert.

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

1. Vertraulichkeit

Zutrittskontrolle:

- Serverinfrastruktur ausschließlich in ISO 27001-zertifizierten Rechenzentren (Hetzner, Nürnberg)
- Kein physischer Zugang Dritter ohne Autorisierung

Zugangskontrolle:

- SSH-Zugang ausschließlich über kryptografische Schlüssel (RSA 4096 Bit / Ed25519)
- Passwort-Authentifizierung deaktiviert
- Root-Login deaktiviert; Verwendung unprivilegierter Systembenutzer mit sudo

Zugriffskontrolle:

- Rollenbasierte Zugriffskontrolle im Datenbanksystem
- Prinzip der minimalen Rechtevergabe (Principle of Least Privilege)
- Separate Datenbankbenutzer je Applikation

Trennungskontrolle:

- Mandantentrennung durch separate Datenbankstrukturen je Auftraggeber (Lizenzkey-basiert)
- Test- und Produktionssysteme logisch und physisch getrennt

Pseudonymisierung:

- Chat-Nachrichten werden vor Weitergabe an KI-Dienste durch den ChatSanitizer-Mechanismus auf erkannte PII-Muster geprüft und ggf. anonymisiert

2. Integrität

Weitergabekontrolle:

- Ausschließliche Nutzung von TLS 1.2+ für alle Datenübertragungen
- API-Kommunikation über HTTPS mit Zertifikatsvalidierung

Eingabekontrolle:

- Input-Validierung und -Sanitierung aller empfangenen Daten
- Protokollierung von Fehlermeldungen und Zugriffsverletzungen

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle:

- Automatisierte Server-Überwachung und Alarmierung
- Regelmäßige Datensicherungen (tägliche Backups, 7-Tage-Aufbewahrung)
- Wiederherstellungsverfahren dokumentiert und regelmäßig getestet

4. Verfahren zur regelmäßigen Überprüfung

Datenschutz-Management:

- Regelmäßige Überprüfung und Aktualisierung dieses AVV bei gesetzlichen Änderungen
- Protokollierung sicherheitsrelevanter Ereignisse

MUSTER

Anlage 3: Unterauftragnehmer

Der Auftragnehmer setzt folgende Unterauftragnehmer ein:

1. Hetzner Online GmbH

Funktion	Hosting und Betrieb der Serverinfrastruktur
Sitz	Industriestr. 25, 91710 Gunzenhausen, Deutschland
Verarbeitungsort	Rechenzentrum Nürnberg, Deutschland (EU)
Vertragsgrundlage	Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO
Verarbeitete Daten	Alle auf den Servern gespeicherten Daten (verschlüsselt übertragen und gespeichert)

2. Anthropic, Inc.

Funktion	KI-Sprachmodell-Inferenz (Generierung von Chat-Antworten)
Sitz	548 Market St, PMB 90375, San Francisco, CA 94104-5401, USA
Verarbeitungsort	USA (Drittland — siehe Anlage 4)
Vertragsgrundlage	Anthropic Data Processing Agreement
Verarbeitete Daten	Chat-Nachrichten der Nutzer (nach PII-Filterung durch ChatSanitizer)

Anthropic verarbeitet gemäß eigener AUP keine übermittelten Daten für das Training von Modellen, sofern keine ausdrückliche Einwilligung vorliegt. Der ChatSanitizer entfernt vor der Übermittlung erkannte personenbezogene Daten (Namen, E-Mail-Adressen, Telefonnummern, Kreditkartennummern, IBAN, IP-Adressen u.a.).

Anlage 4: Drittlandtransfer / Transfer Impact Assessment (TIA)

Empfänger im Drittland

Anthropic, Inc., San Francisco, USA

Rechtsgrundlage des Transfers

Der Transfer in die USA erfolgt auf Basis von **Standardvertragsklauseln (SCCs)** gemäß Art. 46 Abs. 2 lit. c DSGVO (Durchführungsbeschluss EU 2021/914 der Kommission vom 4. Juni 2021) sowie des **EU-U.S. Data Privacy Frameworks (DPF)**, dem Anthropic angehört.

Transfer Impact Assessment

1. Land der Übermittlung und rechtliches Umfeld

Die Daten werden in die Vereinigten Staaten von Amerika übermittelt. Relevant sind insbesondere:

- Der Foreign Intelligence Surveillance Act (FISA), insbesondere Section 702
- Executive Order 12333
- Executive Order 14086 vom Oktober 2022 (Safeguards for U.S. Signals Intelligence Activities)

2. Schutzmaßnahmen

Durch das EU-U.S. Data Privacy Framework und die Executive Order 14086 wurden die folgenden zusätzlichen Garantien etabliert:

- Verhältnismäßigkeit und Notwendigkeit als rechtliche Voraussetzung für Zugriffe durch US-Nachrichtendienste
- Schaffung eines unabhängigen Beschwerdemechanismus (Data Protection Review Court)

Ergänzend gelten folgende technische und organisatorische Maßnahmen:

- Übertragung ausschließlich über TLS 1.2+ verschlüsselte Verbindungen
- PII-Filterung vor Übermittlung (ChatSanitizer)
- API-Key-basierte Authentifizierung (kein Zugriff ohne Authentifizierung)

3. Bewertung

Unter Berücksichtigung des EU-U.S. Data Privacy Frameworks, der SCCs sowie der ergänzenden technischen Maßnahmen (insbesondere PII-Filterung) ist nach Einschätzung des Auftragnehmers ein angemessenes Schutzniveau für die übermittelten Daten gewährleistet. Die übermittelten Daten beschränken sich auf anonymisierte oder pseudonymisierte Chat-Nachrichten; eine Rückführung auf natürliche Personen durch Anthropic ist durch die PII-Filterung erheblich erschwert.

4. Regelmäßige Überprüfung

Dieses Transfer Impact Assessment wird mindestens jährlich sowie bei wesentlichen Änderungen der rechtlichen Grundlage überprüft und ggf. aktualisiert.

MUSTER