

Vertrag zur Auftragsverarbeitung

nach Art. 28 DSGVO

Art. 28 DSGVO stellt spezifische Anforderungen an eine Auftragsverarbeitung. Zur Wahrung dieser speziellen Anforderungen schließen die Vertragsparteien diesen Vertrag zur Auftragsverarbeitung. Er findet Anwendung auf alle Tätigkeiten, die mit dem abgeschlossenen Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers, oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachstehend „Daten“) des Auftraggebers verarbeiten. Es gelten die Begriffsbestimmungen der DSGVO.

1. Vertragsgegenstand und Weisungsrecht des Auftraggebers

- (1) Gegenstand dieses Vertrages sind Leistungen des Auftragnehmers für den Auftraggeber im Bereich der Bereitstellung eines VoiceBots. Bei Änderungen der beauftragten Leistung ist dieser Vertrag zur Auftragsverarbeitung in der Anlage 1 entsprechend anzupassen und zu ergänzen.
- (2) Dem Auftraggeber als verantwortliche Stelle obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung nach der DSGVO.**
- (3) Bei der Erbringung der Leistung erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.
- (4) Die Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt und können vom Auftraggeber in zumindest dokumentiert elektronischem Format durch Einzelweisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. (Art. 28 Abs. 3 lit. a) DSGVO).
- (5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen, ohne dass ihm hierdurch negative Konsequenzen entstehen. Der Auftraggeber ist für die Erteilung rechtsgültiger Weisungen verantwortlich. (Art. 28 Abs. 3 Satz 3 DSGVO).
- (6) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

2. Technisch-organisatorische Maßnahmen

- (1)** Der Auftragnehmer beachtet die gesetzlichen Bestimmungen über den Datenschutz. Eine Weitergabe oder Offenlegung von Informationen des Auftraggebers an Dritte erfolgt ohne eine ausdrückliche Weisung des Auftraggebers nicht. Unterlagen und Daten werden gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik gesichert.
- (2) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO getroffen hat. Hierzu wird auf **Anlage 2** verwiesen.

- (3) Der Auftraggeber überprüft vor der Aufnahme der Datenverarbeitung und sodann regelmäßig die technischen und organisatorischen Maßnahmen des Auftragnehmers. Änderungen an den vereinbarten Sicherheitsmaßnahmen können vorgenommen werden, soweit diese das vertraglich vereinbarte Schutzniveau nicht unterschreiten.

3. Vertraulichkeit

Dem Auftragnehmer und dessen Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer verpflichtet alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden zur Vertraulichkeit. Die Vertraulichkeits-Verpflichtungen gelten auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer.

4. Informationspflichten des Auftragnehmers

- (1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren, soweit sie sich auf diesen Vertrag beziehen. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen.
- (2) Die Meldung über eine Verletzung des Schutzes personenbezogener Daten an den Auftraggeber enthält, soweit möglich, folgende Informationen:
 - a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
 - b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
 - c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (3) Der Auftragnehmer trifft **unverzüglich** die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen, informiert den Auftraggeber und ersucht diesen um weitere Weisungen.
- (4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.
- (5) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 (Art. 28 Abs. 3 lit. e) DSGVO) sowie Art. 32 bis 36 DS-GVO (Art. 28 Abs. 3 lit. f) DSGVO).

5. Kontrollrechte des Auftraggebers

- (1) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.
- (2) Inspektionen durch den Auftraggeber bzw. dessen beauftragten Prüfern, die in keinem Wettbewerbsverhältnis zum Auftragnehmer stehen dürfen, können zu den üblichen Geschäftszeiten und mit einer Vorlaufzeit der Ankündigung von 14 Tagen durchgeführt. Der Auftraggeber führt Kontrollen nur im erforderlichen Umfang durch und stört Betriebsabläufe des Auftragnehmers dabei nur in verhältnismäßiger Weise. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Die Vergütung wird einzelvertraglich vereinbart.

6. Einsatz von Subauftragnehmern

- (1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Hinzuziehung der in **Anlage 3** genannten Subauftragnehmer (Subdienstleister) durchgeführt. Alle zum Vertragsschluss bereits hinzugezogenen und durch den Auftraggeber genehmigten weiteren Auftragsverarbeiter ergeben sich aus der Anlage 3. Der Auftraggeber erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen (Unterauftragnehmer). Wir haben die Verpflichtung, unsere Auftraggeber über die Hinzuziehung oder Änderung weiterer Auftragsverarbeiter zu informieren, wobei die Information schriftlich in Textform ausreichend ist. Weiters schließen wir mit sämtlichen Subauftragnehmern vergleichbare Verträge zur Auftragsverarbeitung ab. Wir unterrichten unsere Auftraggeber mindestens 14 Tage im Voraus in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumen dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können (Einspruchsrecht nach Art. 28 Abs. 2 Satz 2 DSGVO). Das Einspruchsrecht erlischt, sofern Sie nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung über die Änderung oder Hinzuziehung schriftlich Einspruch erhoben haben. Im Falle eines Einspruchs besteht das beiderseitige Recht, den Hauptvertrag sowie diesen Vertrag zur Auftragsverarbeitung mit einer Frist von 3 Monaten zu kündigen.
- (2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt **nicht** vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

7. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

8. Beendigung des Hauptvertrags

- (1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.
- (2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

9. Schlussbestimmungen

- (1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.
- (2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats.
- (3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt und es gelten die gesetzlichen Regelungen des Art. 28 DSGVO.
- (4) Diese Vereinbarung unterliegt deutschem Recht.

Anlagen:

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Subunternehmer

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

<p>Gegenstand der Verarbeitung Art und Zweck der Verarbeitung</p>	<p>Der Auftragsverarbeiter stellt einen Telefon-VoiceBot bereit, der Bewerberdaten im Rahmen eines Erstgesprächs zwischen Bewerbern und dem potenziellen Arbeitgeber erfasst. Der VoiceBot führt die Gespräche automatisch durch, sammelt die relevanten Informationen und überträgt diese, soweit vorhanden, direkt in das Bewerbermanagementsystem des Verantwortlichen und erstellt eine Zusammenfassung des Gesprächs. Der Bot ersetzt dabei eine menschliche Ansprechperson und übernimmt die strukturierte Erfassung von Bewerberdaten im Rahmen des Bewerbungsprozesses. Eine eigenständige Bewertung oder Entscheidung über die Eignung des Bewerbers erfolgt nicht.</p> <p>Zwecke: Automatisierte Erfassung von Bewerberinformationen zur Unterstützung des Bewerbungsprozesses</p>
<p>Art der personenbezogenen Daten</p>	<p>Personenstammdaten: Name, Kontaktdaten wie Telefonnummer</p> <p>Informationen zum Bewerber: beruflicher Werdegang, Qualifikation, Verfügbarkeit, Gehaltsvorstellung, Motivation für die Bewerber, Nachrichten und Informationen aus beantworteten Fragen aus dem jeweiligen Funnel (soweit vorhanden)</p> <p>Technische Daten: Zeitpunkt und Dauer des Gesprächs, Interaktionsdaten, Gesprächsaufzeichnung</p> <p>Die konkret verarbeiteten Daten hängen von den Angaben der Bewerber ab.</p> <p>Werden besondere Kategorien personenbezogener Daten verarbeitet? Je nach Auftrag und Weisung des Auftraggebers. Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, bedarf es einer ergänzenden Vereinbarung.</p>
<p>Kategorien betroffener Personen</p>	<ul style="list-style-type: none"> • Bewerber des Auftraggebers • Mitarbeiter des Auftraggebers

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Nachfolgende Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung wurden implementiert.

Nachfolgende Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung wurden implementiert.

1. Vertraulichkeit

Vertraulichkeit = personenbezogene Daten dürfen unberechtigten Personen oder Organisationen nicht verfügbar gemacht oder offengelegt werden

a. Zutrittskontrolle zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden

= Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verhindern

Externe Termine nur nach Terminvergabe; Zugang ausschließlich mittels Schlüssel

b. Zugangskontrolle zu Datenverarbeitungssystemen

= Maßnahmen, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können

Anmeldung zu Daten Datenverarbeitungssystemen mittels Benutzername und Passwort; Login mit biometrischen Daten, soweit vorhanden; Passwortregelungen: mindestens 8 Zeichen, Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen; Verwendung eines Passwort-Safes; Automatisches Sperren des Bildschirms & Passworteingabe zum erneuten Zugang; Multi-Faktor-Authentifizierung, soweit vorhanden; Einsatz von Anti-Viren-Software; aktive Firewall; Benutzerberechtigungen anlegen (Vergabe nach dem Need-To-Know-Prinzip); Sorgfältige Auswahl von Dienstleistern;

c. Zugriffskontrolle

= Maßnahmen, die es nur Berechtigten erlauben, auf die Daten zuzugreifen, dies betrifft die Verarbeitung, Nutzung und Speicherung (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen)

Berechtigungskonzept (Regelungen zur Beantragung, Freigabe, Umsetzung und Entzug von Berechtigungen); sichere Aufbewahrung von Datenträgern; Mandantenfähigkeit;

d. Trennungskontrolle

= Daten verschiedener Auftraggeber werden getrennt aufbewahrt

logische Trennung (Ordnerstruktur, strukturierte Dateiablage); Führen separater Datenbanken; Mandantenfähigkeit; Berechtigungskonzept; Festlegen von Datenbankrechten

2. Integrität

Wahrung der Richtigkeit, Unverändertheit und Vollständigkeit von personenbezogenen Daten

a. Weitergabekontrolle

= Kein unbefugtes Lesen, Kopieren oder Verändern von Daten bei elektronischen Übertragungen (z. B. E-Mails) oder Transport

Weitergabe ausschließlich nach dem Need-To-Know-Prinzip; Weitergabe von Papierdokumenten in verschlossenen, undurchsichtigen Umschlägen; https-Verschlüsselung auf der Website; Sorgfältige Auswahl von Dienstleistern

b. Eingabekontrolle

= es ist feststellbar, ob, wann und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

differenzierte Benutzerberechtigungen (Lesen, ändern, löschen); Vergabe individueller Benutzernamen; Protokollierung administrativer Tätigkeiten

3. Auftragskontrolle

Es ist ein auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten. Daten des Auftraggebers werden ausschließlich nach dessen Weisungen verarbeitet. Hierzu wurde ein Vertrag zur

Auftragsverarbeitung abgeschlossen. Unterauftragnehmer werden vom Auftraggeber nur nach den Vorgaben der vertraglichen Regelung eingeschaltet.

4. Verfügbarkeit & Belastbarkeit

Schutz gegen Zerstörung und Verlust sowie Gewährleistung der Nutzung von Daten

Feuer-, Wasser- und Rauchmeldeanlagen; Notfallhandbücher; Durchführung von Wiederherstellungstests; Backups; Notfallplan;

5. Regelmäßige Überprüfung, Bewertung & Evaluierung der getroffenen technisch-organisatorischen Maßnahmen

kontinuierliche Überprüfung der TOMs; Führen eines Verarbeitungsverzeichnisses; Bestellung einer Datenschutzbeauftragten – Kontaktdaten: Mag.a iur. Elisa Drescher, office@scaleline-ltd.com; Mitarbeiterschulungen; dokumentierte Prozesse zur Einhaltung der DSGVO etabliert (Auskunftsersuchen fristgerecht beantworten, Verletzung an die Aufsichtsbehörde melden); sorgfältige Auswahl von Dienstleistern; Umsetzung des Zweckbindungsgrundsatzes;

Anlage 3 – Genehmigte Subauftragnehmer

Genehmigte Subauftragnehmer nach 6. dieses Vertrages:

<u>Beauftragtes Unternehmen</u>	<u>Verarbeitungstätigkeit</u>	<u>Verarbeitungsort</u>
<p>Katiba Technology UG (haftungsbeschränkt) Heisinger Straße 12 87437 Kempten</p>	<p>Bereitstellen der Kommunikation über die WhatsApp API sowie Hosting der WhatsApp API</p>	<p>Deutschland</p> <p>Weitere Informationen zu WhatsApp:</p> <p>Irland und Drittländer, in denen verbundene Unternehmen von WhatsApp ihren Sitz haben wie die WhatsApp LLC und Facebook Inc. (Meta Platforms Inc.)</p> <p>WhatsApp LLC, 1601 Willow Road Menlo Park, California 94025 – Zertifizierung nach dem Data Privacy Framework hier abrufen</p> <p>Meta Platforms Inc., Meta Platforms, Inc. 1 Meta Way Menlo Park, California 94025-1453 – Zertifizierung nach dem Data Privacy Framework hier abrufen</p> <p>Data Processing Agreement von WhatsApp Ireland Limited inkl. Auftragsverarbeiter-an-Auftragsver arbeiter Standardvertragsklauseln sowie vollständige Liste mit Subauftragnehmern</p>
<p>OpenAI Ireland Ltd., 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland</p>	<p>Bereitstellen der KI-Technologie, Verarbeiten von Anfragen, Generieren von Antworten.</p>	<p>USA</p> <p>Data Processing Agreement von Open AI inkl. Auftragsverarbeiter-an-Auftragsver arbeiter Standardvertragsklauseln sowie vollständige Liste mit Subauftragnehmern</p>
<p>Eleven Labs Inc., 169 Madison Ave #2484 New York, NY 10016 NYC, USA</p>	<p>Generieren der KI-Stimme</p>	<p>USA</p>

		Data Processing Agreement von ElevenLabs inkl. Auftragsverarbeiter-an-Auftragsverarbeiter Standardvertragsklauseln sowie vollständige Liste mit Subauftragnehmern
Deepgram Inc., 548 Market St, Suite 25104, San Francisco, CA 94104-540, USA	Transkription von Audioinhalten in Text	USA Data Processing Agreement inkl. Standardvertragsklauseln
Celonis, Inc., One World Trade Center 70th Floor New York, NY 10007 United States	Automatisierungen mittels MAKE	USA Data Processing Agreement Aufrechte Zertifizierung nach dem Data Privacy Framework
Supabase Inc., Camden, 3500 S Dupont Hwy, United States	Bereitstellen der Datenbank, technische Infrastruktur für Authentifizierung, Speicherung der Transkripte und der Betroffenenendaten, die Verwaltung der Datenbank für alle Daten	USA Data Processing Agreement inkl. Auftragsverarbeiter-an-Auftragsverarbeiter Standardvertragsklauseln sowie vollständige Liste mit Subauftragnehmern
Twilio Inc, 101 Spear St FL 5 San Francisco, CA 94105, USA	Kommunikationsservice-Provider	USA Data Processing Agreement Aufrechte Zertifizierung nach dem Data Privacy Framework
Vonage Holdings Corp., 101 Crawford's Corner Rd Ste 2416 Holmdel, NJ 07733, USA	Kommunikationsservice-Provider	USA Data Processing Agreement Aufrechte Zertifizierung nach dem Data Privacy Framework
Superpowered Labs Inc., 5 Third Street, 2nd Floor, San Francisco, CA 94103, USA	Bereitstellen der Voice API „VAPI.AI“	USA Data Processing Agreement Aufrechte Zertifizierung nach dem Data Privacy Framework