Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag

(Auftragsverarbeitungsvertrag, Art. 28 DSGVO)

Fassung v1.1 · Stand: 15.10.2026

Auftragsverarbeiter: Islam Aliev, Einzelunternehmen, Feldbergstr. 100, 81825 München

Präambel und Parteien

Auftragsverarbeiter

Islam Aliev, Einzelunternehmen Feldbergstr. 100, 81825 München, Deutschland USt-IdNr. DE328553769 E-Mail: info@anrufpro.de — nachfolgend „**Auftragnehmer**" —

Verantwortlicher

[Firmierung, Rechtsform, Anschrift, USt-IdNr. des Kunden — systemseitig aus den Bestelldaten befüllt] — nachfolgend „**Auftraggeber**" —

Der Auftraggeber hat mit dem Auftragnehmer einen Vertrag über die Nutzung der Plattform und der darüber angebotenen Leistungen geschlossen („**Hauptvertrag**"). Bei der Erbringung dieser Leistungen verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO.

Rangfolge. Diese Vereinbarung geht dem Hauptvertrag und den Allgemeinen Geschäftsbedingungen in datenschutzrechtlichen Fragen vor. Im Übrigen gilt der Hauptvertrag.

Form. Diese Vereinbarung wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO).

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

1. **Gegenstand** der Verarbeitung ist die Erbringung der im Hauptvertrag vereinbarten Leistungen, insbesondere die Entgegennahme, Führung und Dokumentation von Telefongesprächen auf dem Geschäftsanschluss des Auftraggebers durch einen KI-Sprachassistenten sowie die Bereitstellung der daraus gewonnenen Informationen an den Auftraggeber.
2. **Art, Zweck, Datenarten, Kategorien betroffener Personen und Dauer** der Verarbeitung sind in **Anlage A** im Einzelnen beschrieben. Anlage A ist Bestandteil dieser Vereinbarung.
3. Der **Zweck** der Verarbeitung wird allein vom Auftraggeber bestimmt. Der Auftragnehmer verfolgt mit den nach dieser Vereinbarung verarbeiteten Daten **keine eigenen Zwecke**.
4. Die Verarbeitung findet in der Europäischen Union, im Europäischen Wirtschaftsraum sowie — soweit in **Anlage C** ausgewiesen — in Drittländern statt.

5. Die **Dauer** der Verarbeitung entspricht der Laufzeit des Hauptvertrages. Die Pflichten aus § 11 (Löschung und Rückgabe), § 4 (Vertraulichkeit) und § 12 (Nachweise) bestehen darüber hinaus fort.

§ 2 Abgrenzung: eigene Verantwortlichkeit des Auftragnehmers

1. Der Auftragnehmer ist für einen abgegrenzten Teil der bei der Leistungserbringung anfallenden Verarbeitungen **selbst Verantwortlicher** und legt dies hiermit ausdrücklich offen. Das betrifft:

a. Bestands-, Vertrags- und Abrechnungsdaten des Auftraggebers und der für ihn handelnden Personen;

b. **Verbindungs- und Verbrauchsdaten** der über die Plattform abgewickelten Telefonate — beteiligte Rufnummern, Zeitpunkt, Dauer, verbrauchte Minuten, technischer Status —, soweit sie zur Abrechnung, Kapazitätsplanung und Betriebssicherheit des Dienstes des Auftragnehmers erforderlich sind;

c. technische Protokolldaten der Plattform zur Gewährleistung der Systemsicherheit und zur Abwehr von Missbrauch;

d. die Erfüllung eigener gesetzlicher Pflichten des Auftragnehmers, insbesondere steuerrechtlicher Aufbewahrungspflichten (§ 147 AO). Handelsrechtliche Aufbewahrungspflichten nach § 257 HGB bestehen nicht, solange der Auftragnehmer als Kleingewerbetreibender kein Kaufmann ist.

1. **Nicht** von Absatz 1 erfasst sind der **Inhalt** der Gespräche, personenbezogene Daten der anrufenden Personen und die vom Auftraggeber in der Plattform gespeicherten Daten. Für diese ist der Auftragnehmer ausschließlich Auftragsverarbeiter.

2. Der Auftragnehmer verarbeitet die nach dieser Vereinbarung im Auftrag verarbeiteten Daten **nicht** zu eigenen Zwecken. Insbesondere findet **keine** Verwendung statt

a. zum Training, zur Anpassung oder zur Verbesserung von KI-Modellen,

b. zur mandantenübergreifenden Auswertung, Statistik oder Produktentwicklung,

c. zu Zwecken der Werbung oder der Weitergabe an Dritte zu deren Zwecken.

1. Der Auftragnehmer wird die im Auftrag verarbeiteten Daten erst dann zu eigenen Zwecken verarbeiten, wenn hierüber eine **gesonderte, ausdrückliche und gesondert widerrufliche Vereinbarung** mit dem Auftraggeber geschlossen wurde, die den eigenen Zweck, die Rechtsgrundlage, die betroffenen Datenarten und die Information der betroffenen Personen regelt. Eine stillschweigende Erweiterung durch Auslegung dieser Vereinbarung ist ausgeschlossen.

2. Den Parteien ist bekannt, dass ein Auftragsverarbeiter, der unter Verstoß gegen die DSGVO Zwecke und Mittel der Verarbeitung bestimmt, insoweit nach **Art. 28 Abs. 10 DSGVO** als Verantwortlicher gilt.

§ 3 Weisungsrecht *(Art. 28 Abs. 3 S. 2 lit. a DSGVO)*

1. Der Auftragnehmer verarbeitet personenbezogene Daten **ausschließlich auf dokumentierte Weisung** des Auftraggebers. Dies gilt auch für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.
2. **Dokumentierte Weisungen** im Sinne dieser Vereinbarung sind:

a. diese Vereinbarung einschließlich ihrer Anlagen und der Hauptvertrag;

b. die vom Auftraggeber in der Plattform vorgenommenen und gespeicherten **Konfigurationseinstellungen** — insbesondere die Festlegung, welche Angaben im Gespräch erhoben werden, wie lange Daten aufbewahrt werden, an welche Zielsysteme sie übermittelt werden und ob die Aufzeichnungs- und Transkriptionsfunktion nach Anlage A.2 aktiviert ist. Der Auftragnehmer speichert diese Einstellungen versioniert mit Zeitpunkt und handelnder Person und stellt sie dem Auftraggeber auf Anfrage bereit;

c. Einzelweisungen in Textform an info@anrufpro.de oder über die in der Plattform vorgesehene Funktion.

1. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Weisungen, die auf anderem Wege erteilt werden, führt der Auftragnehmer nicht aus.
2. Der Auftragnehmer verarbeitet Daten abweichend von Absatz 1 nur, soweit er hierzu nach dem Recht der Union oder eines Mitgliedstaats verpflichtet ist, dem er unterliegt. In diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen **vor** der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
3. **Hinweispflicht (Art. 28 Abs. 3 S. 3 DSGVO):** Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, teilt er dies dem Auftraggeber **unverzüglich** mit. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung bis zu ihrer Bestätigung oder Änderung durch den Auftraggeber auszusetzen.
4. Der Auftraggeber benennt die zur Erteilung von Weisungen berechtigten Personen: Der Auftraggeber benennt bei Vertragsbeginn eine Ansprechperson mit Name, Funktion und E-Mail-Adresse und teilt Änderungen in Textform mit. Der Auftragnehmer benennt als Ansprechpartner: Islam Aliev, info@anrufpro.de.

§ 4 Vertraulichkeit *(Art. 28 Abs. 3 S. 2 lit. b DSGVO)*

1. Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der jeweiligen Tätigkeit fort.
2. Die Verpflichtung erfasst den Inhaber des Einzelunternehmens persönlich sowie jede weitere natürliche Person, die für den Auftragnehmer Zugang zu personenbezogenen Daten des Auftraggebers erhält, einschließlich freier Mitarbeiterinnen und Mitarbeiter. Die Verpflichtungen werden in Textform erteilt und dokumentiert.

3. Der Auftragnehmer stellt sicher, dass der Zugriff auf personenbezogene Daten des Auftraggebers auf das für die Leistungserbringung Erforderliche beschränkt ist.
4. **Berufsgeheimnisträger.** Ist der Auftraggeber Träger eines Berufsgeheimnisses im Sinne des § 203 StGB — insbesondere Ärztin oder Arzt, Zahnärztin oder Zahnarzt, Angehöriger eines anderen Heilberufs, Rechtsanwältin oder Rechtsanwalt, Steuerberaterin oder Steuerberater —, gilt ergänzend **Anlage E**. Anlage E ist in diesem Fall zwingend zu vereinbaren; ohne sie darf der Dienst für solche Auftraggeber nicht erbracht werden.

---

§ 5 Technische und organisatorische Maßnahmen *(Art. 28 Abs. 3 S. 2 lit. c, Art. 32 DSGVO)*

1. Der Auftragnehmer trifft die zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in **Anlage B** beschrieben.
2. Anlage B beschreibt den Stand bei Vertragsschluss. Der Auftragnehmer darf die Maßnahmen fortentwickeln; das dokumentierte Schutzniveau darf dabei **nicht unterschritten** werden. Wesentliche Änderungen zeigt der Auftragnehmer dem Auftraggeber in Textform an.
3. Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen regelmäßig und dokumentiert die Überprüfung (Art. 32 Abs. 1 lit. d DSGVO). Die Überprüfung erfolgt mindestens Der Auftragnehmer überprüft die Maßnahmen nach Anlage B jährlich sowie anlassbezogen.
4. Anlage B benennt ausdrücklich, welche Maßnahmen der Auftragnehmer selbst erbringt und welche er von Unterauftragsverarbeitern bezieht. Der Auftragnehmer behauptet keine Maßnahmen, die er nicht selbst erbringt.

---

§ 6 Unterauftragsverarbeiter *(Art. 28 Abs. 2 und 4, Art. 28 Abs. 3 S. 2 lit. d DSGVO)*

1. Der Auftraggeber erteilt dem Auftragnehmer eine **allgemeine schriftliche Genehmigung** zur Heranziehung weiterer Auftragsverarbeiter nach Maßgabe dieses Paragraphen. Die bei Vertragsschluss herangezogenen Unterauftragsverarbeiter sind in **Anlage C** abschließend benannt und gelten als genehmigt.
2. Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, teilt er dies dem Auftraggeber **aktiv** mit — per E-Mail an die hinterlegte Adresse und zusätzlich in der Plattform. Die Mitteilung benennt den konkreten Anbieter, dessen Sitz, die vorgesehene Aufgabe, die betroffenen Datenarten und die Grundlage einer etwaigen Drittlandübermittlung. Eine bloße Veröffentlichung auf einer Website genügt nicht.
3. Der Auftraggeber kann der Änderung aus datenschutzrechtlichen Gründen in Textform widersprechen. Die Widerspruchsfrist wird in der Mitteilung genannt. Sie beträgt **mindestens zehn Tage** ab Zugang der Mitteilung, soweit der betreffende Anbieter dem Auftragnehmer eine entsprechende Vorlauffrist einräumt; räumt ein Anbieter dem Auftragnehmer eine kürzere Vorlauffrist ein, gilt diese kürzere Frist, und die Mitteilung weist darauf hin. Der Auftragnehmer leitet die Ankündigung des Anbieters unverzüglich nach ihrem Eingang weiter und gibt die ihm

eingeräumte Vorlauffrist ungekürzt an den Auftraggeber weiter. Der Auftragnehmer sagt keine längere Frist zu, als seine Unterauftragsverarbeiter ihm einräumen; die Fristen der einzelnen Anbieter sind in Anlage C wiedergegeben. Widerspricht der Auftraggeber nicht innerhalb der genannten Frist, gilt die Änderung als genehmigt; hierauf weist die Mitteilung ausdrücklich hin.

4. Im Fall eines begründeten Widerspruchs suchen die Parteien eine einvernehmliche Lösung. Ist eine Leistungserbringung ohne den betreffenden Unterauftragsverarbeiter nicht zumutbar möglich, richten sich die Folgen für den Hauptvertrag — insbesondere ein Recht zur außerordentlichen Kündigung und eine Erstattung im Voraus gezahlter Entgelte — ausschließlich nach den Allgemeinen Geschäftsbedingungen (dort § 8). Diese Vereinbarung trifft hierzu keine eigene Regelung.
5. Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig aus und verpflichtet sie vertraglich auf **dieselben Datenschutzpflichten**, die in dieser Vereinbarung festgelegt sind, insbesondere auf hinreichende Garantien nach Art. 28 Abs. 1 DSGVO. Kommt der Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer dem Auftraggeber gegenüber für dessen Verhalten (Art. 28 Abs. 4 S. 2 DSGVO).
6. Nicht als Unterauftragsverarbeitung im Sinne dieses Paragraphen gelten Nebenleistungen, bei denen kein Zugriff auf personenbezogene Daten des Auftraggebers erfolgt, sowie Dienste, die der **Auftraggeber selbst** durch eine von ihm erteilte Autorisierung anbindet (§ 7).

---

§ 7 Vom Auftraggeber angebundene Dienste

1. Der Auftraggeber kann über die Plattform externe Dienste anbinden, insbesondere Kalenderdienste und Buchungsdienste. Die Anbindung erfolgt durch eine vom Auftraggeber selbst erteilte Autorisierung.
2. Mit der Anbindung weist der Auftraggeber den Auftragnehmer an, die betreffenden Daten an diesen Dienst zu übermitteln. Der Auftraggeber ist dafür verantwortlich, dass für die Nutzung dieses Dienstes und für die Übermittlung eine Rechtsgrundlage besteht und die erforderlichen Verträge mit dem Anbieter geschlossen sind — auch hinsichtlich einer etwaigen Übermittlung in ein Drittland.
3. Anlage C weist diese Dienste gesondert aus.

---

§ 8 Unterstützung bei Betroffenenrechten *(Art. 28 Abs. 3 S. 2 lit. e DSGVO)*

1. Der Auftragnehmer unterstützt den Auftraggeber **mit geeigneten technischen und organisatorischen Maßnahmen** dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO nachzukommen.
2. Der Auftragnehmer kann zu einer benannten Person, soweit anhand von Rufnummer, Name oder Zeitraum identifizierbar:

- die zu ihr gespeicherten Datensätze **suchen und in einem gängigen Format bereitstellen** (Art. 15, 20 DSGVO),

- einzelne Angaben **berichtigen** (Art. 16 DSGVO),
- Datensätze **löschen** oder deren Verarbeitung **einschränken** (Art. 17, 18 DSGVO),
- eine Rufnummer für die weitere Verarbeitung **sperren**.

1. **Tonaufzeichnungen, Transkripte und Zusammenfassungen** entstehen nur, wenn der Auftraggeber die Aufzeichnungs- und Transkriptionsfunktion nach Anlage A.2 aktiviert hat **und** die anrufende Person im Gespräch ausdrücklich eingewilligt hat. Soweit sie vorhanden sind, können sie zu einer benannten Person herausgegeben und gelöscht sowie in ihrer Verarbeitung eingeschränkt werden; eine inhaltliche Berichtigung einer Tonaufzeichnung ist nicht möglich, an ihre Stelle tritt die Löschung oder Einschränkung. Ohne Aktivierung oder ohne Einwilligung existieren weder Aufzeichnung noch Transkript noch Zusammenfassung; herausgegeben, berichtigt, eingeschränkt oder gelöscht werden können dann allein die im Gespräch strukturiert erfassten Angaben und die vom Auftraggeber in der Plattform gespeicherten Daten. Maßgeblich ist die Beschreibung in Anlage A.
2. Der Auftragnehmer bearbeitet Unterstützungsersuchen des Auftraggebers innerhalb von sieben Werktagen
3. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser den Antrag **unverzüglich** an den Auftraggeber weiter und beantwortet ihn nicht selbst. Er teilt der betroffenen Person mit, dass der Auftraggeber Verantwortlicher ist, soweit dies zulässig ist.
4. Ob und in welchem Umfang für die Unterstützung nach diesem Paragraphen ein Entgelt oder ein Aufwandsersatz geschuldet ist, richtet sich ausschließlich nach den Allgemeinen Geschäftsbedingungen (dort § 6). Diese Vereinbarung trifft hierzu keine eigene Regelung.

---

§ 9 Unterstützung bei Sicherheit, Meldepflichten und Folgenabschätzung *(Art. 28 Abs. 3 S. 2 lit. f DSGVO)*

1. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Art. 32 bis 36 DSGVO.
2. **Verletzungen des Schutzes personenbezogener Daten.** Der Auftragnehmer informiert den Auftraggeber über eine Verletzung des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betrifft, **unverzüglich, nachdem ihm die Verletzung bekannt geworden ist** (Art. 33 Abs. 2 DSGVO), in Textform. Der Auftragnehmer gibt die Erstmeldung innerhalb von **24 Stunden nach Kenntniserlangung** ab, gerechnet innerhalb seiner Geschäftszeiten Montag bis Freitag, 9 bis 18 Uhr; fällt der Beginn der Frist außerhalb der Geschäftszeiten, beginnt sie mit deren nächstem Beginn. Eine durchgehend besetzte Überwachung rund um die Uhr besteht nicht (Anlage B.3); eine Verletzung gilt als bekannt geworden, sobald der Auftragnehmer von ihr Kenntnis erlangt hat. Die Meldung enthält, soweit bekannt:

a. eine Beschreibung der Art der Verletzung, soweit möglich mit Kategorien und ungefährer Zahl der betroffenen Personen und Datensätze,
b. den Zeitpunkt oder Zeitraum,
c. die wahrscheinlichen Folgen,

d. die ergriffenen oder vorgeschlagenen Maßnahmen,

e. einen Ansprechpartner.

Liegen nicht alle Angaben vor, meldet der Auftragnehmer zunächst die vorhandenen und ergänzt sie unverzüglich. Die Meldung nennt den Zeitpunkt der Kenntniserlangung des Auftragnehmers, damit der Auftraggeber die Frist des Art. 33 Abs. 1 DSGVO berechnen und einhalten kann.

1. Der Auftragnehmer ergreift unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und dokumentiert den Vorfall.
2. **Datenschutz-Folgenabschätzung.** Der Auftragnehmer stellt dem Auftraggeber die zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlichen Informationen bereit, insbesondere eine Beschreibung der Funktionsweise des eingesetzten KI-Systems, der Datenflüsse, der Unterauftragsverarbeiterkette, der Aufbewahrung und der technischen und organisatorischen Maßnahmen.
3. **Hinweis des Auftragnehmers:** Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder führt in ihrer Liste nach Art. 35 Abs. 4 DSGVO (Version 1.1 vom 17.10.2018) unter Nr. 11 den „Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen" auf, mit dem Einsatzfeld „Kundensupport mittels künstlicher Intelligenz". Der Auftragnehmer weist den Auftraggeber darauf hin, dass für den Einsatz des KI-Sprachassistenten **nach der Auffassung der Aufsichtsbehörden eine Datenschutz-Folgenabschätzung durchzuführen sein dürfte**. Diese Pflicht trifft nach Art. 35 Abs. 1 DSGVO den Auftraggeber als Verantwortlichen. Der Auftragnehmer erteilt hierzu keine Rechtsberatung.

---

§ 10 Pflichten und Rechte des Auftraggebers *(Art. 28 Abs. 3 S. 1 DSGVO)*

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für das Vorliegen einer Rechtsgrundlage nach Art. 6 und, soweit einschlägig, Art. 9 DSGVO.
2. Der Auftraggeber erfüllt die Informationspflichten nach Art. 13 und 14 DSGVO gegenüber den anrufenden Personen und den sonstigen betroffenen Personen. Der Auftragnehmer stellt hierfür Textbausteine bereit (siehe **Anruferinformation**); deren Verwendung entbindet den Auftraggeber nicht von der eigenen Prüfung.
3. Der Auftraggeber legt in der Plattform fest, welche Angaben im Gespräch erhoben werden und wie lange Daten aufbewahrt werden, und bestätigt diese Einstellungen im Onboarding. Diese Bestätigung gilt als dokumentierte Weisung nach § 3 Abs. 2 lit. b.
4. Der Auftraggeber erteilt keine Weisungen, deren Ausführung gegen geltendes Recht verstößt.
5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.
6. Der Auftraggeber führt das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO für die von ihm veranlassten Verarbeitungen. Der Auftragnehmer führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO.

7. **Aufzeichnung von Gesprächen.** Die Aufzeichnungs- und Transkriptionsfunktion (Anlage A.2.2) ist standardmäßig ausgeschaltet. Ihre Aktivierung für den Mandanten des Auftraggebers ist eine dokumentierte Weisung nach § 3 Abs. 2 lit. b. Mit der Aktivierung weist der Auftraggeber den Auftragnehmer an, jede anrufende Person im Gespräch um ihre Einwilligung in die Aufzeichnung zu bitten und Aufzeichnung, Transkript, Zusammenfassung und Auswertung des Gesprächs nur bei ausdrücklich erteilter Einwilligung zu speichern. Der Auftraggeber ist als Verantwortlicher dafür verantwortlich, dass die Einwilligung wirksam ist, dass ein von ihm hinterlegter eigener Wortlaut der Einwilligungsfrage den Anforderungen des Art. 7 DSGVO genügt und dass seine Information der anrufenden Personen den aktivierten Betriebsmodus zutreffend beschreibt. Beide Parteien sind sich einig, dass die Aufnahme des nichtöffentlich gesprochenen Wortes ohne Einwilligung aller Gesprächsbeteiligten nach § 201 Abs. 1 Nr. 1 StGB strafbar ist. Die Aktivierung nimmt der Auftragnehmer auf Weisung des Auftraggebers in Textform vor. Weisung des Auftraggebers in Textform einzuholen und zu protokollieren, bevor geschaltet wird.]`

§ 11 Löschung und Rückgabe *(Art. 28 Abs. 3 S. 2 lit. g DSGVO)*

Es gilt **Anlage D — Löschung und Rückgabe**.

§ 12 Nachweise und Überprüfungen *(Art. 28 Abs. 3 S. 2 lit. h DSGVO)*

1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.
2. Der Nachweis erfolgt in erster Linie durch:

a. diese Vereinbarung nebst Anlagen,
b. die Beschreibung der technischen und organisatorischen Maßnahmen (Anlage B) sowie eine schriftliche Selbstauskunft des Auftragnehmers auf Anfrage,
c. den Auszug aus dem Verzeichnis nach Art. 30 Abs. 2 DSGVO, soweit er den Auftraggeber betrifft,
d. die von den Unterauftragsverarbeitern veröffentlichten Nachweise und Zertifizierungen, soweit vorhanden.

1. **Der Auftragnehmer verfügt selbst über keine Zertifizierung nach Art. 42 DSGVO und über keine Zertifizierung nach ISO 27001, SOC 2 oder einem vergleichbaren Standard.** Er ersetzt das Prüfrecht des Auftraggebers deshalb nicht durch die Vorlage eines Zertifikats.
2. Genügen die Nachweise nach Absatz 2 im Einzelfall nicht, ermöglicht der Auftragnehmer Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer und trägt zu diesen bei. Es gilt:

a. Ankündigung in Textform mit einer Frist von mindestens vier Wochen, außer bei einem konkreten Anlass;
b. Durchführung zu üblichen Geschäftszeiten, ohne unverhältnismäßige Störung des Geschäftsbetriebs;

c. in der Regel höchstens einmal je Kalenderjahr, zusätzlich anlassbezogen;
d. der Prüfer darf kein Wettbewerber des Auftragnehmers sein und ist zur Vertraulichkeit verpflichtet;
e. Betriebs- und Geschäftsgeheimnisse sowie Daten anderer Auftraggeber sind zu schützen.

1. Da der Auftragnehmer über keine eigenen Rechenzentren verfügt, beschränkt sich eine Vor-Ort-Prüfung auf die vom Auftragnehmer selbst betriebenen Arbeitsmittel und Verfahren. Prüfungen bei Unterauftragsverarbeitern richten sich nach deren Prüfkonzepten; der Auftragnehmer unterstützt den Auftraggeber bei entsprechenden Anfragen.
2. Ob für den Aufwand einer Vor-Ort-Prüfung ein Kostenersatz geschuldet ist, richtet sich ausschließlich nach den Allgemeinen Geschäftsbedingungen (dort § 6). Diese Vereinbarung trifft hierzu keine eigene Regelung.

§ 13 Haftung

Für die Haftung der Parteien gelten die Regelungen des Hauptvertrages. Art. 82 DSGVO bleibt unberührt.

§ 14 Schlussbestimmungen

1. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Der Auftragnehmer zeigt beabsichtigte Änderungen aktiv an; sie werden erst mit Zustimmung des Auftraggebers wirksam. Ausgenommen ist die Aktualisierung der Anlagen B und C nach Maßgabe der §§ 5 und 6.
2. Rechtswahl, Gerichtsstand und die Folgen der Unwirksamkeit einzelner Bestimmungen sind ausschließlich in den Allgemeinen Geschäftsbedingungen geregelt (dort § 16) und gelten für diese Vereinbarung entsprechend. Diese Vereinbarung wiederholt sie nicht.
3. Die aktuelle Fassung dieser Vereinbarung ist: **v0.8** [systemseitig zu ersetzen durch die tatsächlich angenommene Fassungskennung; bei jeder Fortschreibung des Dokumentkopfs mitzuziehen].

Anlage A — Beschreibung der Verarbeitung

A.1 Gegenstand

Entgegennahme, Führung und Dokumentation eingehender Telefongespräche auf dem Geschäftsanschluss des Auftraggebers durch einen KI-Sprachassistenten sowie Bereitstellung der daraus gewonnenen Informationen an den Auftraggeber über die Plattform und über die vom Auftraggeber gewählten Zielsysteme.

Ausgehende Anrufe sind enthalten, soweit der Einzelauftrag sie ausweist; es gilt der Leistungsschein Telefonassistent Outbound.

A.2 Art der Verarbeitung — die einzelnen Verarbeitungsvorgänge

A.2.1 Grundbetrieb (alle Tarife; Voreinstellung)

1. Entgegennahme des eingehenden Anrufs und Herstellung der Sprachverbindung.
2. Umwandlung der gesprochenen Sprache in Text (Spracherkennung) zur Führung des Gesprächs.
3. Verarbeitung des Textes durch ein Sprachmodell zur Führung des Gesprächs.
4. Erzeugung synthetischer Sprache als Antwort.
5. Erfassung strukturierter Angaben **während des Gesprächs** über die vom Auftraggeber konfigurierten Funktionen (etwa Name, Rückrufnummer, Anliegen, Terminwunsch, Terminbuchung) und deren Speicherung in der Plattform.
6. Übermittlung an die vom Auftraggeber konfigurierten Zielsysteme (E-Mail, Kalender, Buchungsdienst).
7. Erhebung und Speicherung von Verbindungs- und Verbrauchsdaten — insoweit als eigener Verantwortlicher, siehe § 2.
8. Löschung, soweit für die betreffende Datenart nach A.6 eine Aufbewahrungsdauer konfiguriert und die Löschung nach deren Ablauf aktiviert ist. Für die im Grundbetrieb allein gespeicherten strukturierten Angaben nach Nr. 5 ist nach A.6 bis auf Weiteres keine Frist zugesagt; sie bleiben gespeichert, bis der Auftraggeber sie löscht, längstens bis zum Vertragsende zuzüglich der Fristen nach Anlage D.

Im Grundbetrieb werden **kein Gesprächsaudio, kein Transkript und keine Zusammenfassung gespeichert**. Der aus der Spracherkennung gewonnene Text wird ausschließlich **flüchtig** — für die Dauer der Verarbeitung des laufenden Anrufs — zur Führung des Gesprächs verarbeitet. Dauerhaft gespeichert werden allein die nach Nr. 5 strukturiert erfassten Angaben.

A.2.2 Aufzeichnung und Transkription (nur soweit im Einzelauftrag enthalten und nur nach Aktivierung)

Ob die Aufzeichnungs- und Transkriptionsfunktion enthalten ist, ergibt sich aus dem Einzelauftrag. Ist sie enthalten, ist sie vorhanden, aber **standardmäßig ausgeschaltet**. Sie wird nur wirksam, wenn sie für den Mandanten des Auftraggebers aktiviert ist (§ 10 Abs. 7). Ist sie aktiviert, tritt zu A.2.1 hinzu:

1. **Einwilligungsabfrage.** Der Assistent bittet die anrufende Person im Gespräch mit einem gesprochenen Text um ihre Einwilligung in die Aufzeichnung. Der Auftragnehmer stellt hierfür einen deutschen Standardwortlaut bereit (Anruferinformation, Abschnitt B.4); der Auftraggeber kann einen eigenen Wortlaut hinterlegen, ohne Hinterlegung gilt der Standardwortlaut.
2. **Auswertung der Antwort.** Als Einwilligung gilt allein die ausdrückliche Zustimmung der anrufenden Person. Eine Ablehnung und das Ausbleiben einer Antwort werden **gleich behandelt** — als nicht erteilte Einwilligung. Die Gesprächsführung und die Erfassung strukturierter Angaben nach Nr. 5 sind von der Entscheidung unabhängig.
3. **Ohne Einwilligung:** Es werden **keine** Tonaufzeichnung, **kein** Transkript, **keine** Zusammenfassung und **keine** Auswertung des Gesprächsinhalts gespeichert; die Verarbeitung entspricht A.2.1. Die während des Gesprächs strukturiert erfassten Angaben (Nr. 5) bleiben hiervon unberührt. Ist eine Tonaufzeichnung technisch bereits abgelegt worden, bevor die

Einwilligungsentscheidung vorliegt, wird sie gelöscht, sobald die Entscheidung als nicht erteilt bekannt ist.

4. **Mit Einwilligung:** Gespeichert werden die Tonaufzeichnung, ein Transkript, eine automatisiert erzeugte Zusammenfassung sowie eine strukturierte Auswertung des Gesprächs. Transkript und Zusammenfassung werden **vor der Speicherung** durch ein Verfahren zur Reduktion personenbezogener Angaben geführt; gespeichert wird nur das Ergebnis dieses Verfahrens.
5. **Protokollierung der Einwilligungsentscheidung** (erteilt / abgelehnt / nicht gefragt) je Anruf.

Ausdrücklich nicht Gegenstand der Verarbeitung:

- Keine Tonaufzeichnung, kein Transkript und keine Zusammenfassung ohne aktivierte Funktion **und** ausdrückliche Einwilligung der anrufenden Person.
- Keine biometrische Identifizierung oder Wiedererkennung anrufender Personen anhand der Stimme.
- Keine Emotions- oder Stimmungsanalyse.
- Keine Nutzung der Daten zum Training oder zur Verbesserung von KI-Modellen.

Auch im Grundbetrieb entsteht ein Transkript **kurzzeitig im Verarbeitungsvorgang**; die automatisierte Transkription bleibt eine Verarbeitung personenbezogener Daten. Der Verzicht auf eine Speicherung wird deshalb nicht als „keine Verarbeitung" dargestellt.

Änderungen dieser Beschreibung. Eine über Nummern 1 bis 13 hinausgehende Verarbeitung ist **nicht Gegenstand dieser Vereinbarung** und wird nicht erbracht. Sie setzte eine **Änderung dieser Anlage nach § 14 Abs. 1** und eine entsprechende Anpassung der Anruferinformation voraus. Eine vorweggenommene Genehmigung wird mit dieser Anlage **nicht** erteilt.

A.3 Zweck der Verarbeitung

Die Zwecke bestimmt der Auftraggeber. Typischerweise: Erreichbarkeit des Unternehmens sicherstellen, Anliegen anrufender Personen entgegennehmen und dokumentieren, Termine vereinbaren, Rückrufe veranlassen.

A.4 Arten personenbezogener Daten

- Rufnummer der anrufenden Person sowie Zeitpunkt und Dauer des Anrufs
- Name und weitere Kontaktdaten, soweit im Gespräch genannt
- Inhalt der Äußerungen der anrufenden Person, soweit verarbeitet
- bei aktivierter Aufzeichnungsfunktion und erteilter Einwilligung (A.2.2): Tonaufzeichnung, Transkript, Zusammenfassung und Auswertung des Gesprächs
- bei aktivierter Aufzeichnungsfunktion: die Einwilligungsentscheidung der anrufenden Person je Anruf
- Anliegen, Terminwünsche, Rückrufwünsche und sonstige strukturierte Angaben nach Konfiguration
- Angaben zu Dritten, soweit die anrufende Person sie nennt
- vom Auftraggeber in der Plattform gespeicherte Kontakt- und Kundendaten

Nicht Gegenstand dieser Anlage sind die **Konto- und Zugriffsdaten der Nutzerinnen und Nutzer des Auftraggebers**: Für die Zugangs- und Kontoverwaltung ist der Auftragnehmer nach § 2 Abs. 1 lit. a eigener Verantwortlicher; sie werden nicht im Auftrag verarbeitet.

Besondere Kategorien nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO. Der Auftragnehmer erhebt solche Daten nicht gezielt. Sie können jedoch **beiläufig anfallen**, wenn die anrufende Person sie von sich aus nennt — etwa Gesundheitsangaben bei einer Arztpraxis. Der Auftraggeber ist dafür verantwortlich, dass für eine solche Verarbeitung eine Rechtsgrundlage nach Art. 9 Abs. 2 bzw. Art. 10 DSGVO besteht.

Berufsgeheimnisträger werden nur nach gesonderter Prüfung nach Anlage E als Auftraggeber angenommen.

A.5 Kategorien betroffener Personen

- Personen, die den Geschäftsanschluss des Auftraggebers anrufen — insbesondere dessen Kundinnen und Kunden, Interessenten, Lieferanten, Bewerberinnen und Bewerber
- Dritte, die im Gespräch genannt werden
- Beschäftigte und Beauftragte des Auftraggebers, die die Plattform nutzen
- Kontakte, die der Auftraggeber in der Plattform speichert

A.6 Dauer

Laufzeit des Hauptvertrages. Aufbewahrungsdauer der einzelnen Datenarten, im Rahmen der technisch verfügbaren Optionen:

Datenart	Aufbewahrung
Gesprächsaudio	nur bei aktivierter Aufzeichnungsfunktion und erteilter Einwilligung (A.2.2). Aufbewahrungsdauer **90 Tage ab dem Anruf** (Voreinstellung je Assistent, einstellbar); nach Ablauf Löschung nach Maßgabe der Löschrichtlinie des Assistenten (siehe unten). Ohne Einwilligung: keine Speicherung; eine vor Eingang der Entscheidung abgelegte Aufnahme wird gelöscht, sobald die Entscheidung als nicht erteilt bekannt ist
Transkript, Zusammenfassung, Gesprächsverlauf und Auswertung des Gesprächs	nur bei aktivierter Aufzeichnungsfunktion und erteilter Einwilligung (A.2.2). Aufbewahrungsdauer **90 Tage ab dem Anruf** (Voreinstellung je Assistent, einstellbar); nach Ablauf Löschung nach Maßgabe der Löschrichtlinie des Assistenten (siehe unten)
Während des Gesprächs strukturiert erfasste Angaben (Anliegen, Kontaktangaben, Termindaten)	bis zur Löschung durch den Auftraggeber, längstens bis zum Vertragsende zuzüglich der Fristen nach Anlage D
Einwilligungsentscheidung je Anruf (A.2.2 Nr. 13)	für die Dauer der Speicherung der zugehörigen Aufzeichnung, mindestens jedoch bis zum Ablauf der Fristen nach Anlage D
Vom Auftraggeber in der Plattform gespeicherte Kontakt- und Kundendaten	bis zur Löschung durch den Auftraggeber, längstens bis zum Vertragsende zuzüglich der Fristen nach Anlage D
Technische Protokolldaten der Plattform	Server- und Zugriffsprotokolle 14 Tage; Anwendungsprotokolle 90 Tage
Datensicherungen	35 Tage rollierend
Verbindungs- und Verbrauchsdaten, Abrechnungsunterlagen	eigener Verantwortlicher (§ 2); gesetzliche Aufbewahrungsfristen

Löschrichtlinie des Assistenten. Die Aufbewahrungsdauer der Gesprächsdaten ist je Assistent eingestellt; die Voreinstellung beträgt 90 Tage. Der Auftragnehmer betreibt einen automatisierten Löschlauf, der nach Ablauf der eingestellten Frist Gesprächsaudio sowie Transkript, Zusammenfassung, Gesprächsverlauf und Auswertung aus seinen Systemen entfernt, sofern die Löschung für den Assistenten aktiviert ist; dies ist für Gesprächsaudio und für Transkript nebst personenbezogenen Angaben getrennt einstellbar. **In der Voreinstellung zeichnet der Auftragnehmer kein Gesprächsaudio auf**; solange das so eingestellt ist, entsteht kein Audiobestand und der Löschlauf erfasst insoweit nichts. Die Einstellung nimmt der Auftragnehmer auf Weisung des Auftraggebers in Textform vor.

Die Festlegung der Aufbewahrungsdauer ist eine dem Verantwortlichen vorbehaltene Entscheidung. Der Auftraggeber bestätigt die vorstehenden Werte im Onboarding; diese Bestätigung gilt als dokumentierte Weisung nach § 3 Abs. 2 lit. b. Soweit die Plattform abweichende Fristen zur Auswahl stellt, gilt die vom Auftraggeber gewählte Frist.

Anlage B — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: [Datum] · **Struktur:** Teil 1 beschreibt, was der Auftragnehmer **selbst** tut. Teil 2 benennt, was er von Unterauftragsverarbeitern **bezieht**. Teil 3 nennt die **Grenzen**. Diese Anlage beschreibt ausschließlich tatsächlich umgesetzte Maßnahmen.

B.1 Maßnahmen des Auftragnehmers

Zugangs- und Zugriffskontrolle - Individuelle, personengebundene Konten für alle eingesetzten Dienste und für die Plattform; keine geteilten Zugänge. - Geführte Liste aller Personen mit Zugriff sowie ihrer Berechtigungen; Entzug der Berechtigungen bei Beendigung der Zusammenarbeit, dokumentiert. - Zugriff auf Produktivdaten nur, soweit für Betrieb, Fehlerbehebung oder Support erforderlich. - Rollenkonzept in der Plattform: Kundinnen und Kunden sehen ausschließlich Daten ihres eigenen Mandanten.

Trennung - Mandantentrennung in der Anwendung durch mandantenbezogene Kennzeichnung sämtlicher Datensätze und Durchsetzung auf Anwendungsebene. Die Daten verschiedener Auftraggeber werden in einer gemeinsamen Datenbank gespeichert und **logisch getrennt**: Jeder Datensatz trägt eine Mandantenkennung, und jeder Zugriff ist auf den Mandanten des zugreifenden Kontos eingegrenzt. - Trennung von Produktiv-, Test- und Entwicklungsumgebung; keine Verwendung produktiver personenbezogener Daten zu Test- oder Entwicklungszwecken.

Verschlüsselung und Übertragung - Transportverschlüsselung (TLS) für die öffentlich erreichbaren Verbindungen zur Plattform und zu ihren Programmierschnittstellen (HTTPS-Zugang). Die Verbindung zwischen Anwendung und Objektspeicher verläuft innerhalb des Netzes des Auftragnehmers und ist **nicht zusätzlich transportverschlüsselt**. Die Verbindungen zu den Unterauftragsverarbeitern je Anbieter belegen, bevor sie hier aufgeführt werden.]` - Verschlüsselung der gespeicherten Daten im Ruhezustand, soweit von der eingesetzten Datenbank und dem Objektspeicher bereitgestellt. - Verschlüsselung der Datenträger des eingesetzten Arbeitsgeräts. - Passwörter werden ausschließlich als Hash gespeichert.

Geräte- und Arbeitsplatzsicherheit - Bildschirmsperre, aktuelle Betriebssystem- und Anwendungsstände, aktivierte Firewall auf dem eingesetzten Arbeitsgerät. - Zugangsdaten ausschließlich in einem Passwortmanager; keine Zugangsdaten im Quellcode, in Chatverläufen oder in E-Mails. - Wechsel sämtlicher Zugangsdaten bei Verlust eines Geräts oder bei Beendigung einer Zusammenarbeit.

Protokollierung - Protokollierung administrativer Zugriffe und sicherheitsrelevanter Ereignisse in der Plattform. - Aufbewahrung der Protokolle: Server- und Zugriffsprotokolle 14 Tage; Anwendungsprotokolle 90 Tage

Verfügbarkeit und Wiederherstellbarkeit - Regelmäßige Sicherung der Datenbank. Turnus: täglich. Aufbewahrungsdauer der Sicherungen: 35 Tage rollierend.

Organisation - Verpflichtung auf Vertraulichkeit für alle Personen mit Datenzugriff, in Textform (§ 4). - Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO. - Dokumentiertes Verfahren für Datenschutzverletzungen mit interner Meldefrist, die die Zusage in § 9 Abs. 2 einhält. -

Dokumentiertes Löschkonzept je Datenart. - Führung und Aktualisierung der Unterauftragsverarbeiterliste sowie das Änderungsverfahren nach § 6. - Regelmäßige Überprüfung der Wirksamkeit dieser Maßnahmen nach § 5 Abs. 3.

B.2 Von Unterauftragsverarbeitern bezogene Maßnahmen

Der Auftragnehmer betreibt **keine eigenen Rechenzentren** und erbringt die folgenden Maßnahmen daher nicht selbst, sondern bezieht sie von den in Anlage C genannten Anbietern:

Maßnahme	Erbracht durch
Physische Zutrittskontrolle, Gebäude- und Umgebungssicherheit	Betreiber der Rechenzentren des jeweiligen Anbieters
Redundanz von Strom, Kühlung und Netzanbindung	dieselben
Netzwerksegmentierung und Abwehr von Überlastangriffen auf Infrastrukturebene	Hosting- und Telefonieanbieter
Sicherung und Wiederherstellung auf Infrastrukturebene	Railway (Hosting, Datenbank). Wird der Objektspeicher vom Auftragnehmer selbst betrieben, obliegt dessen Sicherung dem Auftragnehmer (Anlage C, Objektspeicher).
Sicherheit der Sprach- und Modellverarbeitung	ElevenLabs, Google (Gemini, über ElevenLabs), Anthropic
Sicherheit der Zahlungsdatenverarbeitung, PCI-Anforderungen	Stripe

Die von diesen Anbietern veröffentlichten Sicherheitsangaben und Zertifizierungen sind Angaben der jeweiligen Anbieter; der Auftragnehmer macht sie sich nicht als eigene zu eigen und übernimmt keine Gewähr für ihre Richtigkeit.

B.3 Grenzen

Der Auftragnehmer ist ein Einzelunternehmen. Daraus folgt offen benannt:

- **Keine Funktionstrennung** — es gibt eine Person; eine organisatorische Trennung von Entwicklung, Betrieb und Kontrolle ist nicht darstellbar.
- **Keine unabhängige interne Revision.**
- **Keine eigene Zertifizierung** nach ISO 27001, SOC 2 oder Art. 42 DSGVO.
- **Keine durchgehend besetzte Überwachung** rund um die Uhr.
- **Keine eigene Rechenzentrumsinfrastruktur.**

Ausgleichende Maßnahmen: enge Beschränkung des Personenkreises mit Datenzugriff, Protokollierung administrativer Zugriffe, Bezug der Infrastrukturmaßnahmen von spezialisierten Anbietern, kurze Entscheidungswege im Vorfallsfall. Eine Zwei-Faktor-Authentisierung ist in der Plattform **nicht** umgesetzt und wird nicht behauptet.

Art. 32 Abs. 1 DSGVO stellt auf ein dem Risiko **angemessenes** Schutzniveau ab und berücksichtigt dabei ausdrücklich den Stand der Technik und die Implementierungskosten. Diese Anlage beschreibt das tatsächlich erreichte Niveau.

Anlage C — Unterauftragsverarbeiter

Stand: 06.09.2026 — Teil dieser Vereinbarung; maßgeblich ist ausschließlich die Fassungskennung des Gesamtdokuments (Dokumentkopf, § 14 Abs. 3). Eine eigene Fassungskennung führt diese Anlage nicht. Zuletzt inhaltlich geändert: Nr. 3 Aufgabenbeschreibung, Nr. 7 Google, C.3 und C.4 (04.09.2026); Fristenabsatz um Google ergänzt (06.09.2026).

Die Angaben in der Spalte „Grundlage der Drittlandübermittlung" beruhen auf den Auftragsverarbeitungsverträgen der Anbieter, die am **31.08.2026** abgerufen und beim Auftragnehmer abgelegt sind. Der Auftraggeber kann in diese Nachweise auf Verlangen Einsicht nehmen. Der Auftragnehmer ist gegenüber seinen Kunden Auftragsverarbeiter; die nachstehenden Anbieter sind daher **Unterauftragsverarbeiter**, weshalb im Verhältnis zu ihnen regelmäßig **Modul 3** der Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter) einschlägig ist.

C.1 Bei Vertragsschluss eingesetzte Unterauftragsverarbeiter

#	Anbieter	Aufgabe	Verarbeitete Daten	Ort der Verarbeitung	Grundlage der Drittlandübermittlung
1	**ElevenLabs**	KI-Sprachassistent: Spracherkennung, Sprachmodell, Sprachsynthese	Gesprächsinhalt, daraus abgeleiteter Text	USA	**Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914**, in den Auftragsverarbeitungsvertrag einbezogen (dort Ziffer 11.1); anwendbar ist **Modul 3** (Auftragsverarbeiter an Auftragsverarbeiter), da der Auftragnehmer für den Auftraggeber als Auftragsverarbeiter handelt. Anwendbares Recht: Irland. ElevenLabs handelt ausschließlich als Auftragsverarbeiter. Nachweis vom **31.08.2026** (Fassung des Dokuments: 08.04.2026).
2	**Twilio Inc.**, Vereinigte Staaten	Telefonie: Anrufannahme, Vermittlung, Rufnummern	Rufnummern, Verbindungsdaten, Sprachsignal während der Verbindung; ferner Konto- und Nutzungsdaten	USA	Der Auftragsverarbeitungsvertrag sieht eine **Rangfolge** vor: vorrangig der **Angemessenheitsbeschluss EU-US Data Privacy Framework** (Twilio Inc. erklärt sich dort als selbst-zertifiziert), nachrangig die konzerninternen verbindlichen Vorschriften, sodann die **Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914**. Diese sind einbezogen und gelten je nach Datenkategorie in **Modul 1** (soweit Twilio eigener Verantwortlicher ist), **Modul 2** und **Modul 3** — für den Auftragnehmer einschlägig sind **Modul 3** und, für die Daten nach der übernächsten Zeile, **Modul 1**. Anwendbares Recht: Irland. Nachweis vom **31.08.2026** (Fassung des Dokuments: 09.04.2026). **Listung geprüft am 11.09.2026:** „Twilio Inc.", San Francisco, CA, ist auf dataprivacyframework.gov als

#	Anbieter	Aufgabe	Verarbeitete Daten	Ort der Verarbeitung	Grundlage der Drittlandübermittlung
					aktiver Teilnehmer des EU-U.S. Data Privacy Framework gelistet (erfasste Daten: Non-HR Data; Erstzertifizierung 25.10.2016; nächste Fälligkeit 20.04.2027; weitere erfasste Einheit: Stytch). Grundlage der Übermittlung ist damit der **Angemessenheitsbeschluss**; die Standardvertragsklauseln gelten nachrangig und greifen, sobald die Listung entfällt (Mitteilungspflicht von Twilio nach Schedule 3 Ziffer 2.2).
3	**Anthropic**	Sprachmodell für die **nachgelagerte** Verarbeitung nach dem Anruf: strukturierte Auswertung, Erzeugung der Zusammenfassung (nur bei Einwilligung, Anlage A.2.2) sowie Arbeitsabläufe und Assistentenschritte in der Plattform. Die Sprachverarbeitung **während** des Gesprächs erfolgt nicht durch Anthropic, sondern durch Google (Nr. 7)	Gesprächstext, Zusammenfassung, strukturierte Angaben	USA	**Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914**, in den Auftragsverarbeitungsvertrag einbezogen (dort Ziffer I.1); anwendbar ist **Modul 3**. Der Vertrag lässt ausschließlich Modul 2 und Modul 3 zu; Anthropic handelt ausschließlich als Auftragsverarbeiter. Auf den Data Privacy Framework wird nicht abgestellt. Anwendbares Recht: Irland. Nachweis vom **31.08.2026** (Fassung des Dokuments: 24.02.2025). Der Vertrag enthält **keine** ausdrückliche Zusage, dass keine Verwendung zu Trainingszwecken erfolgt; er beschränkt die Nutzung lediglich auf die vereinbarten Geschäftszwecke. Eine ausdrückliche schriftliche Bestätigung ist einzuholen.
4	**SendGrid** (Twilio-Gruppe; geregelt durch denselben Twilio-Auftragsverarbeitungsvertrag)	Versand transaktionaler E-Mails	E-Mail-Adressen, Inhalt der Benachrichtigungen	USA	Wie Nr. 2, **mit einer ausdrücklichen Abweichung:** Die konzerninternen verbindlichen Vorschriften von Twilio gelten für die SendGrid-Dienste **nicht**. Es verbleiben daher der **Data Privacy Framework** und die

#	Anbieter	Aufgabe	Verarbeitete Daten	Ort der Verarbeitung	Grundlage der Drittlandübermittlung
					Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914, **Modul 3**. **Listung geprüft am 11.09.2026:** In der Listung von Twilio Inc. auf dataprivacyframework.gov ist SendGrid **nicht** als eigene erfasste Einheit geführt (einzige weitere Einheit: Stytch). Datenimporteur ist nach dem Vertrag für alle Dienste Twilio Inc. Ferner abweichend: Löschung aus den Sicherungssystemen erst **ein Jahr** nach Vertragsende (statt 60 Tagen bei den übrigen Twilio-Diensten). Nachweis vom **31.08.2026**.
5	**Stripe Payments Europe, Limited**, Irland (Vertragspartner für Konten außerhalb Nord- und Südamerikas); Weitergabe an **Stripe, LLC**, Vereinigte Staaten	Zahlungsabwicklung	Rechnungs- und Zahlungsdaten des Auftraggebers, Zahlungsmittel- und Bankdaten, Gerätekennung und IP-Adresse, Steuernummer, Identitätsnachweise	Irland und **USA** (der Vertrag stellt die Übermittlung an Stripe, LLC in den Vereinigten Staaten ausdrücklich fest)	Der Auftragsverarbeitungsvertrag selbst bezieht keine Standardvertragsklauseln ein, sondern verweist in Ziffer 6.1 auf das **Data Transfers Addendum** (Fassung 18.11.2025, abgerufen 31.08.2026, abgelegt als ../avv-nachweise/2026-08-31_Stripe_DTA.pdf), das dem Auftragsverarbeitungsvertrag vorgeht (Ziffer 7(b)). Das Addendum legt in Ziffer 2 eine **Rangfolge** fest: vorrangig der **Angemessenheitsbeschluss EU-US Data Privacy Framework**, nachrangig die **Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914**. Ziffer 3: Stripe, LLC erklärt sich als selbst-zertifiziert und verpflichtet sich zur unverzüglichen Mitteilung bei Wegfall der Zertifizierung. **Listung geprüft am 11.09.2026:** „Stripe, LLC”,

#	Anbieter	Aufgabe	Verarbeitete Daten	Ort der Verarbeitung	Grundlage der Drittlandübermittlung
					South San Francisco, CA, ist auf dataprivacyframework.gov als **aktiver Teilnehmer** des EU-U.S. Data Privacy Framework gelistet (erfasste Daten: HR Data und Non-HR Data). Datenimporteur ist **Stripe, LLC**, Vereinigte Staaten. Standardvertragsklauseln (Ziffer 4 und 8 des Addendums): Modul 1, 2 und 3 sind einbezogen; nach Ziffer 8.1 gelten Modul 1 und 2, soweit der Kunde von Stripe Verantwortlicher ist, nach Ziffer 8.2 **Modul 3**, soweit er Auftragsverarbeiter ist — das Addendum geht damit über die engere Begriffsdefinition im Auftragsverarbeitungsvertrag (nur Modul 1 und 2) hinaus und hat Vorrang. Ergänzende Zusagen (Ziffer 7): Verschlüsselung bei Übertragung und Speicherung; Widerstand gegen Anfragen nach Section 702 FISA und Anfechtung von Zugriffsverlangen der nationalen Sicherheitsbehörden, soweit rechtlich zulässig; Aufsicht des Datenschutzbeauftragten über internationale Übermittlungen. **Befund aus dem Code (11.09.2026):** Der Auftragnehmer übergibt an Stripe ausschließlich E-Mail-Adresse, Name und interne Mandantenkennung des Auftraggebers; Zahlungsmitteldaten erhebt Stripe selbst. Daten von Anrufern oder Kontakten des Auftraggebers — also Daten, die Gegenstand dieser Vereinbarung sind — gelangen nicht an Stripe. Für

#	Anbieter	Aufgabe	Verarbeitete Daten	Ort der Verarbeitung	Grundlage der Drittlandübermittlung
					die an Stripe übergebenen Daten ist der Auftragnehmer selbst Verantwortlicher. **Rollenverteilung — bestätigt:** Stripe handelt teils als Auftragsverarbeiter, für einen erheblichen Teil der Zahlungsdaten jedoch **als eigener Verantwortlicher** mit alleiniger Entscheidungsbefugnis über Zwecke und Mittel (Betrugsprävention, Sicherheit, Auswahl von Banken und Zahlungsmethodenanbietern, Geldwäsche- und Identitätsprüfungen, gesetzliche Pflichten, Weiterentwicklung eigener Produkte). Für regulierte Leistungen kann Stripe zusätzlich eine Konzerngesellschaft als **gemeinsam Verantwortliche** einsetzen. Insoweit ist Stripe **nicht** Unterauftragsverarbeiter des Auftragnehmers.
6	**Railway Corporation**, 548 Market St PMB 68956, San Francisco, CA 94104, USA	Hosting der Anwendung, PostgreSQL-Datenbank und Bereitstellung der Infrastruktur, auf der der Objektspeicher betrieben wird	sämtliche in der Plattform gespeicherten Daten	**Amsterdam, Niederlande** (Region EU West); Zugriff aus den USA für Betrieb und Support möglich	Standardvertragsklauseln nach **Durchführungsbeschluss (EU) 2021/914**, Modul 2 und Modul 3, im Auftragsverarbeitungsvertrag von Railway einbezogen; Railway ist nach unserer Prüfung vom 15.10.2026 nicht unter dem EU-US Data Privacy Framework zertifiziert. Unterauftragsverarbeiter von Railway: trust.railway.com, Vorankündigung neuer Unterauftragsverarbeiter mindestens zehn Tage.
7	**Google** als Unter-Unterauftragsverarbeiter von ElevenLabs (Nr. 1)	Sprachmodell zur Führung des **laufenden Gesprächs**: Der Auftragnehmer	Gesprächstext während des Anrufs	USA	Google ist **Unterauftragsverarbeiter von ElevenLabs**, nicht des Auftragnehmers. Die Übermittlungsgrundlage

#	Anbieter	Aufgabe	Verarbeitete Daten	Ort der Verarbeitung	Grundlage der Drittlandübermittlung
		konfiguriert für den Assistenten das Modell gemini-2.5-flash; **ElevenLabs ruft dieses Modell auf.** Der Auftragnehmer unterhält keine eigene Vertragsbeziehung zu Google und ruft Google nicht unmittelbar auf			ergibt sich aus der Kette zu ElevenLabs (Nr. 1): Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914, Modul 3. ElevenLabs weist Google in seiner Unterauftragsverarbeiterliste nach.

8 | **DIDWW** [Firmierung und Sitz aus dem Vertrag] | Bereitstellung von Rufnummern und SIP-Anbindung; über diese Anbindung werden die Anrufe zum Sprachdienst (Nr. 1) geführt | Rufnummern, Verbindungsdaten, Sprachsignal während der Verbindung | [Ort aus dem Vertrag] | [Übermittlungsgrundlage aus dem Vertrag; bei Sitz in der EU entfällt sie] |
9 | **sipgate GmbH**, Düsseldorf, Deutschland | Bereitstellung von Rufnummern | Rufnummern, Verbindungsdaten | Deutschland | **Keine Drittlandübermittlung.** |

Anbieter, die zugleich eigene Verantwortliche sind. Twilio (einschließlich SendGrid) und Stripe verarbeiten einen Teil der Daten nach ihren Verträgen **als eigene Verantwortliche** und nicht im Auftrag des Auftragnehmers — Twilio für Konto- und Nutzungsdaten sowie in dem dort genannten Umfang für Inhalte, Stripe für den oben beschriebenen Teil der Zahlungsdaten. Eine gemeinsame Verantwortlichkeit ist bei Twilio ausdrücklich ausgeschlossen. Für diese Verarbeitungen gelten die Datenschutzhinweise des jeweiligen Anbieters; der Auftragnehmer kann sie weder anweisen noch für den Auftraggeber steuern.

Melde- und Widerspruchsfristen bei Wechseln von Unterauftragsverarbeitern (§ 6 Abs. 2 bleibt unberührt; die nachstehenden Fristen sind die des jeweiligen Anbieters gegenüber dem Auftragnehmer): ElevenLabs 30 Tage Vorankündigung; Twilio und SendGrid 30 Tage bei Infrastrukturanbietern, sonst 10 Tage; Anthropic ohne feste Vorlauffrist bei 15 Tagen Widerspruchsfrist; Stripe mindestens 30 Tage; Railway 10 Tage; Google (Nr. 7) ist Unterauftragsverarbeiter von ElevenLabs; insoweit gilt die Vorlauffrist von ElevenLabs (30 Tage).

Räumt ein Anbieter dem Auftragnehmer keine feste Vorlauffrist ein — nach dem heutigen Stand Anthropic —, weist die Mitteilung nach § 6 Abs. 2 ausdrücklich auf die kürzere Frist und deren Grund hin (§ 6 Abs. 3 Satz 3). Für einen Empfänger, dessen Frist in dieser Anlage nicht wiedergegeben ist, wird gegenüber dem Auftraggeber keine Mindestfrist zugesagt.

Objektspeicher. Dateien und Anhänge werden in einem vom Auftragnehmer selbst betriebenen Objektspeicher abgelegt, der auf der Infrastruktur von Railway in Amsterdam, Niederlande, läuft. Ein Speicheranbieter Dritter wird hierfür nicht eingesetzt.

C.2 Vom Auftraggeber selbst angebundene Dienste (§ 7)

Die folgenden Dienste werden **nur** verarbeitet, wenn und soweit der Auftraggeber sie selbst durch eine von ihm erteilte Autorisierung anbindet:

Anbieter	Aufgabe	Verarbeitete Daten	Ort
Cal.com Cloud (app.cal.com)	Terminbuchung	Name, Kontaktdaten, Termindaten	[Sitz und Verarbeitungsort nach Angabe des Anbieters]
Google Calendar (Google)	Kalendereintrag	Name, Termindaten, Anliegen	USA / EU
Microsoft Calendar (Microsoft)	Kalendereintrag	Name, Termindaten, Anliegen	USA / EU

Für diese Dienste bestimmt der Auftraggeber, ob sie eingesetzt werden. Er ist verantwortlich für die Rechtsgrundlage der Übermittlung und für die erforderlichen Verträge mit dem jeweiligen Anbieter.

C.3 Integrierte, nach Angabe des Auftragnehmers nicht produktiv genutzte Dienste

Vapi (Sprachplattform) und **Calendly** (Terminbuchung) sind in der Plattform **technisch integriert und in der Produktionskonfiguration eingerichtet** — Calendly einschließlich einer regelmäßigen automatisierten Abfrage. Nach Angabe des Auftragnehmers werden sie im Produktivbetrieb derzeit **nicht genutzt** und erhalten keine personenbezogenen Daten des Auftraggebers. Diese Dienste werden in der Produktion nicht eingesetzt. Sie sind im System angelegt, aber nur aktiv, wenn der Auftragnehmer die jeweiligen Zugangsdaten hinterlegt; das ist nicht der Fall. Nimmt der Auftragnehmer einen dieser Dienste in Betrieb, gilt das Verfahren nach § 6. **Deepgram** und **Sentry** werden im Produktivbetrieb nicht eingesetzt. Sollte sich an der Nutzung eines dieser Dienste etwas ändern, gilt das Verfahren nach § 6 Abs. 2.

C.4 Werkzeuge zur Auswertung öffentlich zugänglicher Webseiten (Apify, Firecrawl)

Der Auftragnehmer setzt **Apify** und **Firecrawl** für seine **eigene** Neukundenansprache ein; insoweit ist er eigener Verantwortlicher, und die Verarbeitung ist in seiner eigenen Datenschutzerklärung beschrieben. Beide Dienste sind darüber hinaus in der Plattform **als Werkzeuge hinterlegt, die auf Mandantenebene und in Arbeitsabläufen aufrufbar sind**. Werden sie vom Auftraggeber oder für ihn in einem Arbeitsablauf aufgerufen, verarbeiten sie die dabei übergebenen Daten im Auftrag des Auftraggebers; sie sind dann Unterauftragsverarbeiter. Diese Werkzeuge werten öffentlich zugängliche Webseiten aus. Sie werden nur aufgerufen, wenn ein Arbeitsablauf des Auftraggebers sie ausdrücklich einsetzt; die übergebenen Angaben bestimmt dabei der Auftraggeber.

Anlage D — Löschung und Rückgabe *(Art. 28 Abs. 3 S. 2 lit. g DSGVO)*

D.1 Wahlrecht des Auftraggebers

Nach Beendigung des Hauptvertrages löscht der Auftragnehmer sämtliche im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie **nach Wahl des Auftraggebers** zurück und löscht vorhandene Kopien. Der Auftraggeber teilt seine Wahl spätestens **30 Tage nach Vertragsende** in Textform mit. Trifft er keine Wahl, werden die Daten gelöscht.

D.2 Rückgabe

Auf Verlangen stellt der Auftragnehmer die Daten in einem gängigen, maschinenlesbaren Format bereit — Format: CSV und JSON, Tonaufzeichnungen als MP3. Die Bereitstellung erfolgt innerhalb von zehn Werktagen nach Zugang des Verlangens über einen abgesicherten Abrufweg.

D.3 Löschfristen nach Datenart

Datenart	Löschung
Tonaufzeichnung, Transkript, Zusammenfassung, Gesprächsverlauf und Auswertung des Gesprächs (nur bei aktivierter Funktion und Einwilligung, Anlage A.2.2)	im laufenden Vertrag nach Ablauf der je Assistent eingestellten Aufbewahrungsdauer, Voreinstellung **90 Tage ab dem Anruf**, nach Maßgabe der Löschrichtlinie des Assistenten (Anlage A.6); nach Vertragsende unabhängig davon spätestens **30 Tage** nach Vertragsende, vorbehaltlich eines Rückgabeverlangens nach D.2
Während des Gesprächs strukturiert erfasste Angaben in der Plattform	spätestens **30 Tage** nach Vertragsende, vorbehaltlich eines Rückgabeverlangens nach D.2; im laufenden Vertrag nach Anlage A.6
Dateien im Objektspeicher (einschließlich Tonaufzeichnungen)	spätestens **30 Tage** nach Vertragsende, vorbehaltlich D.3a und eines Rückgabeverlangens nach D.2
Vom Auftraggeber in der Plattform gespeicherte Kontakt- und Kundendaten	spätestens **30 Tage** nach Vertragsende, vorbehaltlich D.3a und eines Rückgabeverlangens nach D.2
Datensicherungen	mit dem Ablauf des Sicherungszyklus, spätestens 35 Tage rollierend. Bis dahin werden die Daten in den Sicherungen für die produktive Nutzung gesperrt und nur im Fall einer Wiederherstellung berührt; nach einer Wiederherstellung wird die Löschung unverzüglich nachgeholt.
Verbindungs- und Verbrauchsdaten sowie Abrechnungsunterlagen	**nicht** nach dieser Anlage — hierfür ist der Auftragnehmer eigener Verantwortlicher (§ 2) und unterliegt gesetzlichen Aufbewahrungspflichten

Die **Konten und Zugangsdaten der Nutzerinnen und Nutzer** sind nicht Gegenstand dieser Anlage; für sie ist der Auftragnehmer nach § 2 Abs. 1 lit. a eigener Verantwortlicher. Der

Auftragnehmer löscht sie mit Vertragsende; ein für den Abruf nach § 8a Abs. 2 der Allgemeinen Geschäftsbedingungen erforderlicher Zugang bleibt für die Dauer des Abrufzeitraums bestehen.

Vorrang des Übergangs- und Abrufzeitraums (D.3a). Sämtliche Fristen dieser Anlage D.3, die an das Vertragsende anknüpfen, stehen unter dem Vorbehalt des Übergangs- und Abrufzeitraums nach § 8a der Allgemeinen Geschäftsbedingungen. Verlangt der Auftraggeber nach D.1/D.2 oder nach § 8a AGB eine Bereitstellung oder Übertragung der Daten, so beginnt die Löschfrist dieser Anlage erst mit dem Ablauf des Abrufzeitraums nach § 8a Abs. 2 und, falls ein Übergangszeitraum nach § 8a Abs. 4 vereinbart oder benannt ist, erst mit dessen Ablauf. Die Verarbeitung ist in diesem Zeitraum auf die Bereitstellung, Übertragung und Sicherung der Daten sowie auf die Erfüllung gesetzlicher Pflichten beschränkt; eine darüber hinausgehende Verarbeitung findet nicht statt. Der Zeitraum endet spätestens mit dem in § 8a Abs. 4 genannten Höchstzeitraum.

Rechtsgrundlage: Die Fortdauer der Speicherung beruht in diesem Zeitraum auf der ausdrücklichen Weisung des Auftraggebers nach § 3 dieses Vertrages; Art. 28 Abs. 3 S. 2 lit. g DSGVO stellt die Löschung ausdrücklich unter das Wahlrecht des Verantwortlichen und steht einer weisungsgemäßen Rückgabephase nicht entgegen.

Reichweite dieser Fristen. Die Fristen dieser Anlage gelten für die **vom Auftragnehmer selbst gehaltenen Kopien** — Plattformdatenbank, Objektspeicher und eigene Datensicherungen. Für Kopien, die bei Unterauftragsverarbeitern liegen, gilt D.5.

Der Auftragnehmer sagt keine sofortige Löschung aus Datensicherungen zu. Diese Angabe ist bewusst so gefasst, weil Sicherungen zyklisch überschrieben werden und eine punktgenaue Löschung darin technisch nicht darstellbar ist.

D.4 Aufbewahrung kraft Gesetzes

Soweit das Recht der Union oder eines Mitgliedstaats die Aufbewahrung verlangt, unterbleibt die Löschung insoweit. Der Auftragnehmer teilt dem Auftraggeber Art und Umfang solcher Aufbewahrung mit und beschränkt die Verarbeitung auf den gesetzlich vorgesehenen Zweck.

D.5 Unterauftragsverarbeiter

Der Auftragnehmer veranlasst nach Vertragsende die Löschung bei den Unterauftragsverarbeitern und weist sie auf Verlangen nach, soweit ihm dies möglich ist. **Der Zeitpunkt der Löschung bei einem Unterauftragsverarbeiter richtet sich nach dessen in Anlage C wiedergegebenen Vertragsbedingungen, nicht nach D.3.** Nach dem Stand der Anlage C bedeutet das insbesondere: ElevenLabs schuldet bei Self-Serve-Leistungen keine Löschung binnen einer Frist, sondern behält sich die Löschung nach 180 Tagen Inaktivität lediglich vor; SendGrid löscht Sicherungskopien erst ein Jahr nach Vertragsende; Stripe nennt keine Frist; die Löschfrist bei Railway richtet sich nach dessen Auftragsverarbeitungsvertrag, die bei Google (Nr. 7) ebenfalls. Der Auftragnehmer sagt keine Löschfrist zu, die ein Unterauftragsverarbeiter ihm nicht schuldet.

D.6 Nachweis

Der Auftragnehmer bestätigt die vollständige Löschung auf Verlangen in Textform.

Anlage E — Ergänzende Regelungen für Berufsgeheimnisträger

> **Nur zu vereinbaren**, wenn der Auftraggeber Berufsgeheimnisträger im Sinne des § 203 StGB ist. Andernfalls entfällt diese Anlage ersatzlos.

1. Der Auftragnehmer und die für ihn tätigen Personen werden als **sonstige mitwirkende Personen** im Sinne des § 203 Abs. 3 S. 2 StGB tätig. Sie werden ausdrücklich zur Geheimhaltung verpflichtet und über die strafrechtlichen Folgen einer Pflichtverletzung belehrt. Die Verpflichtung erfolgt in Textform und wird dokumentiert.
2. Der Auftragnehmer trägt dafür Sorge, dass auch die von ihm herangezogenen weiteren mitwirkenden Personen zur Geheimhaltung verpflichtet werden (§ 203 Abs. 4 S. 2 Nr. 2 StGB). Die Kenntnisnahme von Geheimnissen wird auf das für die Leistungserbringung Erforderliche beschränkt.
3. Diese Anlage wird **nur nach gesonderter anwaltlicher Prüfung im Einzelfall** vereinbart. Für Rechtsanwälte (§ 43e BRAO) und Steuerberater (§ 62a StBerG) gelten zusätzliche Anforderungen an den Dienstleistervertrag; § 43e Abs. 4 BRAO lässt im Ausland erbrachte Dienstleistungen nur zu, wenn der dortige Geheimnisschutz dem inländischen vergleichbar ist. Da an der Leistungserbringung Unterauftragsverarbeiter mit Sitz in den Vereinigten Staaten beteiligt sind (Anlage C), ist diese Voraussetzung vor dem ersten Vertragsschluss mit einem Berufsgeheimnisträger gesondert zu prüfen. Ohne diese Prüfung wird diese Anlage nicht vereinbart.
4. Der Auftraggeber bleibt dafür verantwortlich, dass die Offenbarung gegenüber dem Auftragnehmer für die Inanspruchnahme der Leistung erforderlich ist (§ 203 Abs. 3 S. 2 StGB).
