

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen	und
Denker & Ludwig GbR Konrad-Adenauer-Straße 7 26935 Stadland	Kunde
vertreten durch	vertreten durch
im Folgenden: Auftragnehmer	im Folgenden: Auftraggeber

- Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“)

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

- Gegenstand und Dauer der Verarbeitung

2.1. Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Erhebung/Erfassung, Speicherung, Verwendung etc. von Personenstammdaten, Kommunikationsdaten, Gesprächsinhalten (Audio-Streams, Gesprächsaufzeichnungen — soweit vom Auftraggeber aktiviert —, Transkripten und KI-Zusammenfassungen), Termindaten sowie von Anrufern im Gespräch mitgeteilten Informationen — einschließlich Gesundheitsdaten im Sinne des Art. 9 DSGVO, soweit Anrufer diese mitteilen — von Anrufern, Kunden, Patienten und Interessenten des Auftraggebers zum Zwecke der automatisierten Telefonannahme und -assistenz (Entgegennahme und Führung von Telefongesprächen, Terminvereinbarung und -verwaltung, Weiterleitung, Versand von Benachrichtigungen per E-Mail/SMS/WhatsApp) sowie der Bereitstellung eines Dashboards zur Einsicht und Verwaltung.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag XYZ „SpeakKI-Dienstleistungsvertrag“ (Order-Form nebst AGB und Leistungsbeschreibung) vom [Datum] (im Folgenden „Hauptvertrag“).

2.2. Die Verarbeitung beginnt am [Datum] und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

- Art und Zweck der Datenverarbeitung

3.1. Der Auftragnehmer erbringt digitale Dienstleistungen und erhält unter gewissen Umständen Zugriff auf den elektronischen Bestand an personenbezogenen Daten und Datensätzen von Kunden des Auftragsgebers.

3.2 Die Verarbeitung durch den Auftragnehmer erfolgt in der Art der Entgegennahme und Führung von Telefongesprächen mittels eines KI-gestützten Sprachassistenten, der Erhebung, Speicherung, Transkription und automatisierten Auswertung (Zusammenfassung, Kategorisierung) von Gesprächsinhalten, der Terminvereinbarung und -verwaltung, der Weiterleitung von Anrufen sowie des Versands von Benachrichtigungen (E-Mail/SMS/WhatsApp) für den Auftraggeber

Der Auftraggeber ist ... [geschäftliche Tätigkeit des Auftraggebers].

3.3. Die Verarbeitung dient dem Zweck des/der der automatisierten telefonischen Erreichbarkeit (KI-Telefonassistenz), Terminvereinbarung und -verwaltung sowie Benachrichtigung von Anrufern und Kunden für den Auftraggeber und erfolgt aufgrund dessen Interesses an durchgehender telefonischer Erreichbarkeit, Entlastung der eigenen Mitarbeiter, effizienter Terminorganisation und lückenloser Dokumentation eingehender Anliegen

3.4. Es werden folgende Kategorien personenbezogener Daten verarbeitet:

- Allgemeine Personendaten (Name, ggf. Geburtsdatum)
- Kommunikationsdaten (Telefonnummer, E-Mail-Adresse, ggf. Anschrift)
- Gesprächsinhalte (Audio-Streams, Gesprächsaufzeichnungen — soweit vom Auftraggeber aktiviert —, Transkripte, KI-generierte Zusammenfassungen und Kategorisierungen)
- Termin- und Vorgangsdaten (vereinbarte Termine, Anliegen, Rückrufwünsche)
- Gesundheitsdaten (Art. 9 DSGVO), soweit Anrufer diese im Gespräch mitteilen (insbesondere bei Auftraggebern aus dem Gesundheitswesen)

3.5. Von der Verarbeitung betroffen sind:

- Anrufer und Angerufene des Auftraggebers (Kunden, Patienten, Interessenten)
- Mitarbeiter des Auftraggebers (Nutzerkonten der Plattform, Ansprechpartner)
- Kontakte des Auftraggebers (Telefonbucheinträge)

• Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.8. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

4.10. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU, des EWR oder in Staaten, für die ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO gilt. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

• Technische und organisatorische Maßnahmen

5.1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen (technische und organisatorische Maßnahmen) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

5.2. Die Maßnahmen gemäß vorheriger Ziffer können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

5.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet. Die Verarbeitung im Homeoffice ist zulässig, sofern die in Anlage 1 festgelegten Schutzmaßnahmen eingehalten werden, insbesondere die Nutzung ausschließlich geschäftlich verwendeter, vollverschlüsselter Endgeräte mit Bildschirmsperre, Multi-Faktor-Authentifizierung sowie der Zugriff auf Produktionssysteme ausschließlich über gesicherte Verbindungen (SSH/VPN).

5.7. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

5.8. Der Auftraggeber ist berechtigt, die Erfüllung der Pflichten durch den Auftragnehmer, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihre Wirksamkeit, unter Vorankündigung mit angemessener Frist zu kontrollieren und zu überprüfen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu diesem Zweck und für die Dauer der Kontrolle Zugang zu allen relevanten Räumlichkeiten sowie Einsicht in und Zugriff auf alle für die Prüfung erforderlichen Dokumente und Systeme zu verschaffen.

• Regelungen zur Berichtigung, Löschung und Sperrung von Daten

6.1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

6.2 Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

- **Unterauftragsverhältnisse**

7.1. Die Beauftragung von Subunternehmern durch den Auftragnehmer ist zulässig. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers jederzeit Auskunft über die gegenwärtig und in der Vergangenheit für die Auftragsverarbeitung eingesetzten Subunternehmer zu erteilen und Einsicht in mit diesen Subunternehmern über die weitere Datenverarbeitung im Auftrag geschlossene Verträge zu gewähren.

7.2. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.3. Weitere Subbeauftragung durch den Subunternehmer sind nach den Maßgaben der Ziffer 7.1. zulässig.

7.4. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.5. Die Beauftragung von Subunternehmern im Sinne von Ziffer 7.1. und Ziffer 7.3., die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU, des EWR oder Staaten erbringen, für die ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO gilt, ist nur bei Beachtung der in Ziffer 4.10. dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

7.6. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig angemessen zu überprüfen und die Ergebnisse zu dokumentieren. Die Dokumentation ist dem Auftraggeber auf dessen Verlangen hin vorzulegen.

7.7. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7.8. Zurzeit sind die in Anlage 2 mit Namen und Anschrift bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang betraut. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

7.9. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

- **Rechte und Pflichten des Auftraggebers**

8.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

8.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

8.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen im Sinne der Ziffer 5 sowie ihre Wirksamkeit, beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

8.5. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

- **Mitteilungspflichten**

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat unverzüglich, spätestens innerhalb von 48 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

9.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

- Weisungen

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

10.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt oder zu einer Haftung des Auftragnehmers führen kann. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10.5. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.

- Beendigung des Auftrags

11.1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse X.

11.2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber auf Verlangen vorzulegen.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

- Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

- Haftung

13.1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

13.2. Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit personenbezogene Daten in seiner Verantwortung vom Auftragnehmer unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragnehmer ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

13.3. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13.4. Die Ziffer 13.3 gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

- Sonderkündigungsrecht

14.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

14.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

- Sonstiges

15.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

15.2. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

15.3. Für Nebenabreden ist die Schriftform erforderlich.

15.4. Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

.....	
Ort, Datum	Ort, Datum
Auftragnehmer	Auftraggeber

• **Anlage 1 – technische und organisatorische Maßnahmen**

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

• **Zutrittskontrolle**

- Die Verarbeitung erfolgt ausschließlich in einem zertifizierten Rechenzentrum (Hetzner Online GmbH, Standort Nürnberg, Deutschland; ISO-27001-zertifiziert). Die physische Zutrittskontrolle zum Rechenzentrum obliegt dem Rechenzentrumsbetreiber.
- Arbeitsplätze: ausschließlich geschäftlich genutzte Endgeräte mit vollständiger Datenträgerverschlüsselung (FileVault).
- Automatische Bildschirmsperre auf allen Arbeitsgeräten; keine Nutzung der Arbeitsgeräte durch Dritte.

• **Zugangskontrolle**

- Jedes System, mit dem personenbezogene Daten verarbeitet werden, ist mittels Benutzerauthentifizierung geschützt; sämtliche Konten und Schlüssel sind personengebunden (keine geteilten Zugänge).
- Passwort-Manager mit starken, einmaligen Passwörtern; Multi-Faktor-Authentifizierung auf allen kritischen Diensten (Hosting, Code-Repository, Cloud-Dienste, Telefonie).
- Server-Zugang ausschließlich per SSH-Schlüssel; Passwort-Login ist deaktiviert.
- Die Produktionsdatenbank ist nicht öffentlich erreichbar; Zugriff ausschließlich über SSH-Tunnel oder VPN. Firewall auf Serverebene.

• **Zugriffskontrolle**

Rollenbasiertes Berechtigungsmodell in der Plattform (Administrator/Mitglied). Sämtliche Datenzugriffe sind mandantenbezogen beschränkt: Jede Abfrage ist an die Organisation des angemeldeten Benutzers gebunden (organisationsbezogene Zugriffskontrolle auf Datenbankebene, im Rahmen eines Sicherheitsaudits überprüft).

• **Transport-/Weitergabekontrolle**

- Sämtliche Datenübertragungen erfolgen transportverschlüsselt (TLS); interne Dienste kommunizieren über gesicherte Verbindungen.
- Zugriff auf Gesprächsaufzeichnungen ausschließlich über zeitlich befristete, signierte URLs (presigned URLs); Datenträger in mobilen Endgeräten sind verschlüsselt.

- **Eingabekontrolle**

Änderungen an Konfiguration und Daten werden systemseitig protokolliert (Anwendungs- und Server-Logs); Änderungen am Quellcode unterliegen der Versionskontrolle mit personengebundenen Commits.

- **Auftragskontrolle**

Subunternehmer werden ausschließlich mit Auftragsverarbeitungsvertrag eingesetzt (siehe Anlage 2); Trainingsnutzung durch KI-Dienstleister ist vertraglich bzw. technisch ausgeschlossen (Opt-out). Die Auftragskontrolle wird mindestens einmal jährlich durchgeführt.

- **Verfügbarkeitskontrolle**

- Tägliche, verschlüsselte Datensicherungen; Speicherung der Sicherungen innerhalb der EU (Hetzner, Deutschland).
- Monitoring und Alarmierung der Produktionssysteme; Wiederherstellungskonzept (Backup & Recovery).
- Betriebssystem- und Sicherheitsupdates werden zeitnah eingespielt; Firewall auf Server- und Geräteebe.

- **Trennungsgebot**

Daten, welche zu unterschiedlichen Zwecken erhoben, verarbeitet oder genutzt werden, werden getrennt gespeichert. Die Trennung erfolgt:

- Logische Mandantentrennung auf Datenbankebene: sämtliche Datensätze sind einer Organisation zugeordnet, alle Abfragen organisationsgebunden
- Getrennte Speicherpfade je Organisation im Objektspeicher (Gesprächsaufzeichnungen)
- Trennung von Produktions-, Staging- und Entwicklungsumgebung mit jeweils eigenen Zugangsdaten
- Getrennte Telefonie-Anbindungen (SIP-Trunks) und Agent-Instanzen je Umgebung

- **Datenträgervernichtung**

- Es erfolgt keine papiergebundene Verarbeitung von Auftragsdaten.
- Löschung elektronischer Daten durch sichere Lösungsverfahren; die Entsorgung physischer Datenträger im Rechenzentrum obliegt dem zertifizierten Rechenzentrumsbetreiber.

- **Fernwartung**

Es erfolgt keine Fernwartung durch andere Unternehmen.

11. Verfügbarkeit und Belastbarkeit

a) Für alle internen System ist eine Eskalationskette definiert, welche vorgibt, wer im Fehlerfall zu informieren ist, um das jeweilige System schnellstmöglich wiederherzustellen.

b) Verfügbarkeitskontrolle:

1. Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten
2. Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
3. Redundante Datenhaltung und tägliche, verschlüsselte Sicherungen auf Serverebene (Backup- und Recovery-Konzept)

Anlage 2- Gegenwärtige Subunternehmer

Der Auftragnehmer bedient sich zur Erbringung der Datenverarbeitungen im Auftrag zum Zeitpunkt des Vertragsschlusses der folgenden Subunternehmer:

1. Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland — Hosting der gesamten Infrastruktur (Anwendung, Datenbank, Objektspeicher, Media-Server); Verarbeitungsort: Rechenzentrum Nürnberg (DE).
2. Deepgram, Inc., 548 Market St, San Francisco, CA 94104, USA — Sprach-zu-Text-Transkription; Verarbeitung über EU-Regional-Endpoint (EU-Region); Absicherung: Auftragsverarbeitungsvertrag mit EU-Standardvertragsklauseln; Trainingsnutzung ausgeschlossen (Opt-out).
3. ElevenLabs, Inc., 169 Madison Ave, New York, NY 10016, USA — Sprachsynthese (Text-zu-Sprache); Absicherung: Auftragsverarbeitungsvertrag mit EU-Standardvertragsklauseln (Bestandteil der ElevenLabs Terms of Service, elevenlabs.io/dpa); Trainingsnutzung ausgeschlossen (Opt-out).
4. Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (Vertex AI) — Sprachmodell-Inferenz; Verarbeitungsregion: EU; Absicherung: Google Cloud Data Processing Addendum.
5. Twilio Ireland Limited, 25-28 North Wall Quay, Dublin 1, Irland — Telefonie-Anbindung (SIP-Trunk); Absicherung: Auftragsverarbeitungsvertrag mit EU-Standardvertragsklauseln.
6. Sendinblue SAS („Brevo“), 106 Boulevard Haussmann, 75008 Paris, Frankreich — Versand von Transaktions-E-Mails; Verarbeitungsort: EU.
7. seven communications GmbH & Co. KG, Willestr. 4-6, 24103 Kiel, Deutschland — SMS-Versand; Einsatz erst ab Aktivierung der SMS-Funktion durch den Auftraggeber.
8. Meta Platforms Ireland Limited, Merrion Road, Dublin 4, Irland (WhatsApp Business Platform) — WhatsApp-Nachrichtenversand; Einsatz erst ab Aktivierung der WhatsApp-Funktion durch den Auftraggeber; Absicherung: Auftragsverarbeitungsvertrag mit EU-Standardvertragsklauseln bzw. EU-US Data Privacy Framework.
10. OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, Irland — Sprachmodell-Inferenz (Gesprächsführung; Einsatz wahlweise als primäres Sprachmodell oder als Ausfallsicherung) sowie ergänzende KI-Funktionen; Verarbeitung: EU-Region (Data Residency); Absicherung: Auftragsverarbeitungsvertrag mit EU-Standardvertragsklauseln; kein Training mit Kundendaten (API-Standard).

Die jeweils aktuelle Liste der Subunternehmer ist unter <https://speakki.de/subprozessoren> abrufbar. Änderungen werden dem Auftraggeber mindestens 30 Tage vor Wirksamwerden in Textform angekündigt.

Anlage 3- Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

1. Weisungserteilung

Zur Erteilung von Weisungen befugt sind auf Seiten des Auftraggebers dessen gesetzliche Vertreter sowie sämtliche Benutzer, die der Auftraggeber in der SpeakKI-Plattform mit der Rolle „Administrator“ angelegt hat. Weisungen erfolgen in Textform (z. B. E-Mail) oder über die dafür vorgesehenen Funktionen der SpeakKI-Plattform; über die Plattform vorgenommene Konfigurationsänderungen gelten als dokumentierte Weisungen.

2. Weisungsentgegennahme

Zur Entgegennahme von Weisungen befugt sind auf Seiten des Auftragnehmers die Gesellschafter der Denker & Ludwig GbR (Felix Denker und Marvin Ludwig), erreichbar unter privacy@speakki.de.