Vereinbarung zur Auftragsverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung (siehe Anhang 3)

- nachfolgend **„Leistungsvereinbarung**“ -

zwischen dem
Kunden (näher spezifiziert auf Seite 8)

- nachfolgend **„Verantwortlicher**“ -

und

SpeechMind GmbH vertreten durch Richard Fankhänel

- nachfolgend **„Auftragsverarbeiter**“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhaltsverzeichnis

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 – DSGVO) sowie der einschlägigen nationalen Datenschutzgesetze zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

Für öffentliche Stellen der Länder gilt ergänzend das jeweils anwendbare Landesdatenschutzgesetz (LDSG), soweit dessen Vorschriften Anwendung finden.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung personenbezogener Daten bestimmen sich nach der Leistungsbeschreibung in der jeweils gültigen Fassung, die Bestandteil dieser Vereinbarung ist (siehe Anhang 3).
Die Nichteinhaltung der in dieser Vereinbarung festgelegten Pflichten sowie der sich aus Art. 28 DSGVO ergebenden Anforderungen stellt einen schweren Vertragsverstoß dar.

(2) Folgende Datenarten bzw. -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

- Identifikationsdaten: Name, E-Mail-Adresse, optional Telefonnummer
- Audio- und Videodaten: Aufzeichnungen von Sitzungen oder Besprechungen
- Transkribierte Gesprächsinhalte: automatisch erzeugte Textfassungen aus Audio-/Videodaten
- Meeting-Metadaten: Datum, Dauer, Teilnehmer, ggf. Titel oder Zweck des Meetings

(3) Der Kreis der betroffenen Personen umfasst insbesondere:

- Teilnehmerinnen und Teilnehmer von Meetings bzw. Besprechungen, deren Inhalte verarbeitet werden,
- Moderatorinnen und Moderatoren bzw. Sitzungsleitungen,
- Personen, deren Namen, Stimmen oder Äußerungen im Rahmen der Verarbeitung erfasst werden sowie
- Nutzende der SpeechMind Software.

(4) Eine Übersicht der beauftragten Unterauftragnehmer ist in Anhang 2 aufgeführt.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Gemäß § 4 Abs. 2 Satz 3 dieser Vereinbarung unterstützt der Auftragsverarbeiter den Verantwortlichen dabei mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche oder elektronische Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden. Weisungsberechtigt sind bei Einzelplatzlizenzen der jeweilige Nutzer selbst, bei Organisationslizenzen die Geschäftsführung des Verantwortlichen, der/die Datenschutzbeauftragte sowie die in der Software-Anwendung als Administratoren benannten und vom Verantwortlichen autorisierten Personen.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der Europäischen Union statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen und ist nur dann zulässig, wenn das betreffende Drittland über ein adäquates Datenschutzniveau verfügt, welches durch die Europäische Kommission mittels des sogenannten Angemessenheitsbeschlusses gemäß art. 44 und 45 DSGVO festgestellt wurde. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitungen bleiben unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

(10) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Kunde verantwortlich.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen sowie mit den datenschutztechnischen Bestimmungen vertraut sind und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung. Der Auftragsverarbeiter unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person und unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. f DSGVO)..

(3) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht .

(5) Im Falle einer Inanspruchnahme des Verantwortlichen durch eine Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten bestmöglich zu unterstützen.

(6) Nur für Unterstützungsleistungen, die auf ein schuldhaftes Fehlverhalten des Verantwortlichen zurückzuführen sind, kann der Auftragsverarbeiter eine zusätzliche angemessene Vergütung beanspruchen.

Kontaktdaten Datenschutzbeauftragter SpeechMind GmbH:

Name: Titus Hartmann
E-Mail: titus@speechmind.de
Telefon: +49 (0) 351 / 89732833-3

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang 1 „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung. Der Auftragsverarbeiter hat darüber hinaus sämtliche angemessene Sicherheitsmaßnahmen unter der Berücksichtigung des Stands der Technik zu ergreifen

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen" festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen unaufgefordert und unverzüglich mitzuteilen.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutzfolgenabschätzung i.S.d. Art. 35 DSGVO), hinsichtlich etwaiger Melde- oder Genehmigungsverfahren, sowie bei vorherigen Konsultationen der Aufsichtsbehörde (Art 36 DSGVO) benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO.

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Gewährleistung eines angemessenen Schutzniveaus nach Art. 32 DSGVO, bei der Meldung und Benachrichtigung bei Datenschutzverletzungen nach Art. 33 und 34 DSGVO, bei der Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO sowie bei der vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO.

Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gemäß § 3 dieses Vertrages durchführen.

Die durch die Unterstützungsleistungen entstehenden Kosten trägt der Verantwortliche, es sei denn, die Unterstützung wurde durch

einen Verstoß des Auftragsverarbeiters gegen gesetzliche oder vertragliche Pflichten erforderlich; in diesem Fall trägt der Auftragsverarbeiter die Kosten.

Bei aufsichtlichen Maßnahmen beim Verantwortlichen hat der Auftragsverarbeiter ihn in Bezug auf die bei ihm für den Verantwortlichen durchgeführten Verarbeitungstätigkeiten bestmöglich zu unterstützen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen unaufgefordert vorzulegen. Der Auftragsverarbeiter verzichtet ausdrücklich auf die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB hinsichtlich des Anspruches auf Rückgabe der verarbeiteten Daten und der zugehörigen Datenträger. Dies gilt auch für alle Kopien und Reproduktionen der Daten.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend den jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen. [Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind in der Anlage 2 im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden]. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Verantwortliche zustimmt. Die Regelung in § 3 Abs. 8 dieser Vereinbarung gilt entsprechend.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortliche berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Schlussbestimmungen

(1) Der Verantwortliche ist berechtigt, diese Vereinbarung und/oder die Leistungsvereinbarung fristlos und außerordentlich zu kündigen, sofern der Auftragsverarbeiter einen erheblichen Datenschutzverstoß begeht, insbesondere wenn er gegen die in dieser Vereinbarung festgelegten Pflichten verstößt oder die Weisungen des Verantwortlichen nicht befolgt.
Geringfügige Verstöße sind vom Auftragsverarbeiter unverzüglich zu beheben. Der Verantwortliche setzt dem Auftragsverarbeiter hierfür eine angemessene Frist. Erfolgt die Behebung nicht fristgerecht, ist der Verantwortliche ebenfalls zur außerordentlichen Kündigung berechtigt.
Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn die Daten des Verantwortlichen durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim Auftragsverarbeiter gefährdet werden. Der Auftragsverarbeiter informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Verantwortlichen liegt.

Unterschriften

Verantwortlicher

Unterschrift:	_____
Unternehmen:	_____
Name:	_____
Titel:	_____
Datum:	_____

Auftragsverarbeiter

Unterschrift:	
Unternehmen:	**SpeechMind GmbH, Königstr. 4, 01097 Dresden**
Name:	**Richard Fankhänel**
Titel:	**Geschäftsführer SpeechMind**
Datum:	**20.02.2026**

Anhang 1 „Technisch-organisatorische Maßnahmen“

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	Zutrittskontrollsystem (mit Datenbank mit Protokollierung der Schlüsselbenutzungen), Schlüsselvergabe, Türsicherung
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Passwörter mit Mindestanforderungen (8 Zeichen, 1 Nummer, 1 Kleinbuchstaben, 1 Großbuchstaben, 1 Sonderzeichen) organisationsweit und in der Anwendung, Zwei-Faktor-Authentifizierung für die Cloud, Verwendungen von AWS Cognito als Identitätsspeicher mit verschlüsselter Übertragung der Daten (TLS1.2) und verschlüsselter Speicherung der Zugänge im Ruhezustand bei Nutzerdaten
3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Die Zugriffskontrolle wird durch ein zentrales rollenbasiertes Berechtigungsmanagement (RBAC) mit minimalen Zugriffsrechten sichergestellt. Die Verwaltung der Berechtigungen erfolgt ausschließlich durch autorisierte Administratoren nach dem Need-to-Know-Prinzip. Alle administrativen Zugriffe und Änderungen an Berechtigungen werden systemseitig protokolliert. Die Datenübertragung erfolgt durchgehend verschlüsselt, und die Zugriffsberechtigungen werden regelmäßig durch die IT-Administration überprüft und angepasst.

4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Die Übertragung aller personenbezogenen Daten erfolgt ausschließlich verschlüsselt über HTTPS mittels TLS 1.2/1.3. Die interne Datenspeicherung und -übertragung ist durch Verschlüsselung nach aktuellem Stand der Technik geschützt. Datenübermittlungen an Dritte werden dokumentiert und erfolgen nur auf Basis einer rechtlichen Grundlage. Die Übermittlungswege werden regelmäßig auf ihre Sicherheit überprüft und bei Bedarf aktualisiert.
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Alle Eingaben, Änderungen und Löschungen von personenbezogenen Daten werden im System automatisch protokolliert (Logging). Diese Protokollierung umfasst den Zeitpunkt, die Art der Aktion und den durchführenden Mitarbeiter. Die Protokolldaten sind vor nachträglicher Manipulation geschützt und können nur von autorisierten Administratoren eingesehen werden. Wartungs- und Servicezugriffe durch IT-Dienstleister werden ebenfalls vollständig protokolliert und dokumentiert.
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter (AVV mit Cloud-Dienstleistern)
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	AWS/ OVH Cloud stellt mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren. Von der Datenbank wird 1 Mal täglich ein Backup gemacht. Das Recovery-Konzept wird einmal pro Quartal geübt.
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet, Mandantenfähigkeit, Funktionstrennung zwischen Produktions- /Testumgebung durch Staging Server.
9.	**Regelmäßige Untersuchung zur Wirksamkeit der Maßnahmen**	Die Wirksamkeit der Technischen und Organisatorischen Maßnahmen wird mindestens einmal jährlich überprüft. Diese Überprüfung erfolgt durch interne Audits und Penetrationstests, die durchgeführt werden. Alle Feststellungen aus den Prüfungen werden dokumentiert,

		bewertet und führen bei Bedarf zu Maßnahmen zur kontinuierlichen Verbesserung.
10.	**Incident-Response-Management**	Ein Incident-Response-Management-Prozess ist etabliert, der folgende Punkte umfasst: ● **Meldung und Dokumentation:** Sicherheitsvorfälle werden über ein zentralisiertes System (Ticketing-System) erfasst. ● **Untersuchung:** Vorfälle werden von dem Entwicklungsteam analysiert, und entsprechende Gegenmaßnahmen werden eingeleitet. ● **Eskalation:** Kritische Vorfälle werden direkt an die Geschäftsführung und ggf. an die zuständigen Datenschutzbehörden gemeldet. ● **Lessons Learned:** Nach jedem Vorfall werden Analysen durchgeführt, und Präventivmaßnahmen werden implementiert. ● **Schulungen:** Alle notwendigen Mitarbeiter werden regelmäßig geschult, um potenzielle Sicherheitsvorfälle frühzeitig zu erkennen und korrekt zu melden.
11.	**Privacy by Design / Privacy by Default**	**Privacy by Design:** Datenschutzanforderungen werden bereits in der Konzeptions- und Entwicklungsphase aller Produkte und Systeme berücksichtigt. Es erfolgt eine systematische Risikoanalyse, und technische Schutzmaßnahmen (z. B. Pseudonymisierung, Verschlüsselung) werden direkt implementiert. **Privacy by Default:** Alle Systeme und Anwendungen sind standardmäßig so konfiguriert, dass sie nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten verarbeiten. Es werden keine unnötigen Daten erhoben oder gespeichert. Benutzer können Datenschutzpräferenzen einfach und intuitiv einstellen.

(2) Änderungen, die den Datenschutz betreffen, werden dem Vertragspartner per E-Mail mitgeteilt. Wenn gewünscht, kann gemeinsam eine erneute Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien in dem Fall vorgenommen werden.

(3) Weiter Vorkehrungen:

- Die von SpeechMind genutzten Cloud Anbieter AWS, OVH und Azure sind nach den folgenden Normen zertifiziert:
  - ISO 27001 für technische Maßnahmen
  - ISO 27017 für Cloud-Sicherheit
  - ISO 27018 für Cloud-Datenschutz
  - SOC 1, SOC 2 und SOC 3, PCI DSS Level 1,
  - BSIs Cloud Computing Compliance Controls Catalogue (C5)
  - ENS Hoch

- Alle Sprachdaten werden mittels Server-side encryption mit 256-bit Advanced Encryption Standard (AES-256) verschlüsselt abgespeichert
- Es besteht die Möglichkeit der Überwachung von Berechtigungen und auch die Möglichkeit, als Administrator Rechte zu entziehen.
- Einem Benutzer, der nicht mehr der Organisation angehört, kann der Zugriff auf die Daten entzogen werden.

- Die Daten Übertragbarkeit nach DSGVO wird mittels Exports von JSON Dateien gewährleistet (Exportfunktion). Der Auskunftsanspruch aus der DSGVO ist damit bei entsprechendem Wunsch erfüllbar.
- Lösch- und Sperrfristen sind sichergestellt. Bei Kundenwunsch können entsprechende Löschfristen realisiert werden.
- Es werden keine Kundendaten zum Training des KI-Modells verwendet.

§ 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

4.1 Datenschutzschulungen und Geheimhaltung
Jährliche Datenschutzschulungen werden für alle Mitarbeitenden durchgeführt, um das Bewusstsein und Verständnis für den Umgang mit personenbezogenen Daten gemäß den aktuellen Datenschutzgesetzen zu fördern.
Alle Mitarbeiter sind vertraglich zur Geheimhaltung und zum vertraulichen Umgang mit allen sensiblen und personenbezogenen Daten verpflichtet.

4.2 Benennung und Rolle des Datenschutzbeauftragten (DSB)
Ein Datenschutzbeauftragter ist offiziell und freiwillig ernannt, um die Einhaltung der Datenschutzvorschriften zu überwachen. Diese Maßnahme ist sowohl im Vertrag fixiert als auch in den TOMs dokumentiert, um die aktive Rolle des DSB in unseren Datenschutzpraktiken zu unterstreichen.

4.3 Evaluierung und Implementierung einer Datenschutzmanagement Software
Die Evaluierung zur Auswahl einer geeigneten Datenschutzmanagement Software wird durchgeführt, um unsere Datenschutzverfahren zu unterstützen und zu optimieren. Die Entscheidung und Implementierung werden dokumentiert und in die laufenden Prozesse integriert.

4.4 Zentrale Dokumentation
Ein zentrales Verfahrensverzeichnis sowie umfassende Regelungen zum Datenschutz werden stetig geführt und aktualisiert. Diese Dokumentation ist zugänglich für den Datenschutzbeauftragten und autorisierte Personen, um eine konsistente Handhabung personenbezogener Daten zu gewährleisten.

4.5 Datenschutzfolgenabschätzung (DSFA)
Die DSFA kann als Grundlage für die interne Abschätzung des Unternehmens von SpeechMind erfragt werden.

4.6 Etablierung von Prozessen bei Datenschutzvorfällen und Auskunftsersuchen
Es sind klare Prozesse für den Umgang mit Datenschutzpannen und Auskunftsersuchen etabliert. Diese beinhalten die unverzügliche Meldung an den Datenschutzbeauftragten und die Bearbeitung der Vorfälle innerhalb von 72 Stunden.

4.7 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Anhang 2 „Verzeichnis der Unterauftragnehmer der KI-gestützte

Protokollierungssoftware SpeechMind Studio"

Die personenbezogenen Meetingdaten unserer Kunden werden DSGVO-konform verarbeitet. Die Datenverarbeitung erfolgt ausschließlich auf EU-Servern (Frankfurt/Westeuropa). Kein Drittlandtransfer. AWS und Microsoft sind DPF-zertifiziert gemäß Art. 45 DSGVO.

Empfänger:

OVH GmbH
Oskar-Jäger-Str. 173/K6,
50825 Köln
Deutschland
USt-IdNr.: DE245768940
Handelsregister: Amtsgericht Köln - HRB 122481
E-Mail: kundendienst@ovh.de

Amazon Web Services EMEA SARL
38 Avenue John F. Kennedy
1855 Luxembourg
Luxembourg
E-Mail: aws-EU-privacy@amazon.com

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Deutschland
USt-IdNr.: DE 129 415 943
Handelsregister: Amtsgericht München: HRB 70438
E-Mail: kunden@microsoft.com

Zweck der Verarbeitung	Kategorie personen-bezogene Daten	Empfänger	Land Empfänger	Frist Löschung Daten	Technische/Organisatorische Maßnahmen zum Schutz	Link
Speicherung der Protokolldaten (Text) in Datenbank	Bezug auf Nutzerdaten, Unternehmensdaten, Name, E-Mail etc. Weitere Betroffene: Meetingteilnehmer mit Bild- und Ton-Daten	OVH Cloud (Gemanagte Datenbank)	Deutschland	Bei Löschen des Projektes	Serverstandort Frankfurt, OVH unterliegt der DSGVO	OVH Cloud
Bereitstellung von Diensten oder Funktionen	Bezug auf Nutzerdaten, Unternehmensdaten, Name, E-Mail, Textdaten etc.	OVH Cloud (Kubernetes Cluster)	Deutschland	Temporäre Speicherung, Löschung am Ende des Zwecks ihrer Verarbeitung	Serverstandort Frankfurt, OVH unterliegt der DSGVO	OVH Cloud

Speicherung Sprachspur	Text- und Sprachdaten Betroffene: Meetingteilnehmer mit Bild- und Ton-Daten	AWS (S3 Speicher, Lambda Funktion)	Deutschland	Löschfristen einstellbar für 30/60/90 Tage sowie unbegrenzt oder beim Löschen des Projektes oder Protokolls	Serverstandort Frankfurt, AWS SSE-S3 Verschlüsselung, Kommunikation mittels HTTPS	AWS
Nutzerdatenbank	Name, Email, Telefonnummer, Unternehmensname	AWS (Cognito)	Deutschland	Am Ende des Zwecks ihrer Verarbeitung	Kommunikation mittels HTTPS, Data is encrypted at rest	AWS Cognito
Verarbeitung der Sprachspur	Text- und Sprachdaten Betroffene: Meetingteilnehmer mit Bild- und Ton-Daten	Microsoft Azure	Westeuropa (EU)	Temporäre Speicherung (max. 48 Stunden)	Authentifizierung	MS Azure
Bereitstellung von KI Funktionen	Textdaten	Microsoft Azure (Azure OpenAI)	Westeuropa (EU)	Kein persistente Speicherung	Authentifizierung	Azure OpenAI

Anhang 3 “Leistungsbeschreibung für KI-gestützte Protokollierungssoftware SpeechMind Studio”

1. Gegenstand der Leistung

Die vorliegende Leistungsbeschreibung regelt die Bereitstellung und Nutzung der KI-gestützten Software „SpeechMind Studio“, die darauf ausgelegt ist, aus Audioaufnahmen detaillierte schriftliche Protokolle zu generieren. Diese Software verwendet fortschrittliche Algorithmen des maschinellen Lernens und der Spracherkennung, um Sprache effektiv in Text umzuwandeln.

2. Dauer der Auftragsverarbeitung

Der Auftrag zur Verarbeitung der Daten wird für den Zeitraum der aktiven Nutzung der Software durch den Kunden erteilt. Eine automatische Verlängerung des Nutzungszeitraumes erfolgt montalich oder jährlich entsprechend der vereinbarten Lizenz, sofern nicht mindestens ein Monate vor Ablauf des Vertragsjahres schriftlich gekündigt wird.

3. Umfang der Datenverarbeitung

Die Software verarbeitet die folgenden Arten von Daten:

- Audioaufnahmen: Gesprochene Inhalte in Meetings, Konferenzen, Sitzungen oder ähnlichen Veranstaltungen.
- Metadaten: Dauer der Aufnahmen, Datum und Uhrzeit der Erstellung, beteiligte Sprecher (sofern identifizierbar).

4. Art der Datenverarbeitung

Die Datenverarbeitung umfasst:

- Automatische Transkription von Audio zu Text.
- Erkennung und Differenzierung zwischen verschiedenen Sprechern (Speaker Diarization).
- Anreicherung des Transkripts mit Zeitstempeln und Sprecherkennung.
- Möglichkeit zur manuellen Überprüfung und Korrektur der automatisch erstellten Transkripte durch den Nutzer.
- Identifikation von Aufgaben (sofern ausgewählt).
- Erstellung eines Ergebnisprotokolls in Stichpunkten und thematisch gegliedert (sofern ausgewählt).
- Erstellung eines Verlaufsprotokolls in indirekter Rede und im Konjunktiv (sofern ausgewählt).
- Beantworten von Fragen basierend auf dem zugrunde liegenden Transkript durch eine digitale Assistenz.

5. Zweck der Datenverarbeitung

Der Zweck der Datenverarbeitung durch “SpeechMind Studio“ besteht darin:

- Effiziente Dokumentation und Archivierung von gesprochenem Wort in schriftlicher Form.
- Erleichterung der Informationsaufbereitung und -analyse.
- Unterstützung bei der Compliance mit Dokumentationspflichten.
- Bereitstellung eines Tools zur Verbesserung der Zugänglichkeit und Barrierefreiheit von gesprochenen Informationen.

6. Datenschutz und Sicherheit

Die Software gewährleistet die Einhaltung der geltenden Datenschutzgesetze. Alle Daten werden verschlüsselt übertragen und gespeichert. Die Verarbeitung der personenbezogenen Daten erfolgt ausschließlich in Rechenzentren, die den strengen EU-Datenschutznormen entsprechen. Löschfristen sind einstellbar.