Vereinbarung über die

Verarbeitung von Daten im Auftrag (AV-Vereinbarung)

Zwischen dem **Kunden**

- Auftraggeber oder Hauptauftragnehmer nachfolgend **„Auftraggeber“** -

und **DNAnalytics UG (haftungsbeschränkt)**

- Auftragnehmer oder Unterauftragsverarbeiter nachfolgend **„Auftragnehmer“** -

gemeinsam auch „Parteien“

wird vereinbart:

Präambel

Der Auftragnehmer übernimmt für den Auftraggeber die Durchführung von Analysen von vom Auftraggeber durchgeführten und aufgezeichneten Coaching-Sessions mittels der Software DNACoachingAssist. In diesem Zuge werden dem Auftragnehmer personenbezogene Daten aus der Sphäre des Auftraggebers (insb. Daten des Klienten) offengelegt und der Auftragnehmer muss diese personenbezogenen Daten verarbeiten. Um diese Datenverarbeitung im Einklang mit geltendem Datenschutzrecht durchführen zu können, vereinbaren die Parteien die nachfolgende Vereinbarung über die Verarbeitung von Daten im Auftrag (nachfolgend „AV-Vereinbarung“).

Auftraggeber ist – je nach Verarbeitungssituation –datenschutzrechtlicher Verantwortlicher oder selbst (erster) Auftragsverarbeiter für einen anderen Verantwortlichen, also Hauptauftragnehmer. Auftragnehmer ist entsprechend entweder (erster) Auftragsverarbeiter oder Unterauftragsverarbeiter. Mit Abschluss dieser AV-Vereinbarung soll eine datenschutzkonforme Datenverarbeitung durch Auftragnehmer als erster Auftragsverarbeiter und im Unterauftrag ermöglicht werden. Die Parteien bezwecken mit dieser AV-Vereinbarung die datenschutzrechtlich konforme Einbindung von Auftragnehmer in die Datenverarbeitung von Auftraggeber, gleich ob Auftraggeber selbst Verantwortlicher ist oder Auftragnehmer in eine bestehende Verarbeitungskette zwischen datenschutzrechtlich Verantwortlichem und Hauptauftragnehmer eingebunden werden soll. Alle Regelungen dieser AV-Vereinbarung sind im Lichte dieses Vertragszweckes zu interpretieren.

1. **Gegenstand und Merkmale der Datenverarbeitung im Auftrag**

1.1. Diese AV-Vereinbarung regelt den Umgang mit personenbezogenen Daten durch den Auftragnehmer im Rahmen von der Nutzung des Auftraggebers von DNACoachAssist. Die AV-Vereinbarung gilt hinsichtlich des Umgangs mit personenbezogenen Daten vorrangig vor den anderen vertraglichen Regelungen und neben bestehenden Geheimhaltungspflichten. Gesetzliche Aufbewahrungspflichten von Auftragnehmer bleiben unberührt.

1.2. Gegenstand, Umfang, Art und Zweck der Datenverarbeitung, die Art der personenbezogenen Daten sowie die Kategorien der Betroffenen werden in **Anlage 1** zu dieser AV-Vereinbarung spezifiziert, soweit sie nicht in den anderen vertraglichen Regelungen bereits festgelegt sind. Bei etwaigen Widersprüchen gehen die Regelungen dieser AV-Vereinbarung und all ihrer Teile anderen vertraglichen Regelungen vor.

1.3. Diese Vereinbarung regelt ggf. auch die Datenverarbeitung im Unterauftragsverarbeitungsverhältnis. Um den datenschutzrechtlichen Anforderungen gerecht zu werden, gelten alle Rechte des Auftraggebers gemäß dieser AV-Vereinbarung für den jeweiligen datenschutzrechtlich Verantwortlichen („Verantwortlicher“). Dies gilt auch ohne eine entsprechende ausdrückliche Bezugnahme in den jeweiligen Klauseln.

1.4. Die Verarbeitung und Nutzung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland findet nur statt, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

2. **Pflichten von Auftraggeber**

2.1. **Verantwortlichkeit für Datenverarbeitung**

Auftraggeber ist für die Verarbeitung und gegenüber Dritten für die Einhaltung der Vorschriften der Datenschutzgesetze datenschutzrechtlich verantwortlich, soweit er nicht selbst als Auftragsverarbeiter tätig wird. Auftraggeber hat die datenschutzrechtliche Zulässigkeit der Auftragsverarbeitung und des Auftrages eigenverantwortlich zu beurteilen. Ist Auftraggeber der Meinung, die Verarbeitung durch Auftragnehmer verstoße gegen Pflichten von Auftraggeber, so hat er Auftragnehmer hierauf hinzuweisen und eine rechtskonforme Datenverarbeitung durch entsprechende Weisungen sicherzustellen.

2.2. **Mitteilungs- und Weisungspflichten**

Im Falle eines unmittelbaren Auskunftsverlangens, Hinweises, einer Warnung oder Anweisung einer Aufsichtsbehörde nach Art. 58 DSGVO unterstützt Auftraggeber Auftragnehmer. Auftraggeber wird sicherstellen, dass dem behördlichen Verlangen in Übereinstimmung mit dieser AV-Vereinbarung Folge geleistet werden kann.

3. Pflichten von Auftragnehmer

3.1. Bindung an Weisungen

3.1.1. Auftragnehmer wird die Daten von Auftraggeber ausschließlich im Rahmen dieser AV-Vereinbarung und nach dessen Weisungen verarbeiten. Diese AV-Vereinbarung räumt Auftraggeber ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung zu. Dieses Weisungsrecht wird durch Einzelweisungen konkretisiert. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

3.1.2. Auskünfte an Dritte oder die Betroffenen wird Auftragnehmer nur nach vorheriger Weisung durch Auftraggeber erteilen. Dies gilt nicht, soweit Auftragnehmer nach geltendem Recht zur Herausgabe verpflichtet ist. Ziff. 6.4 bleibt unberührt.

3.1.3. Auftraggeber erteilt Weisungen, indem die jeweiligen Funktionen der bereitgestellten Software genutzt werden, mit denen die Datenverarbeitung gesteuert werden kann (etwa die Löschfunktion bezüglich der transkribierten Coaching-Sessions). Alle Weisungen außerhalb dieser Funktionalitäten sind zu dokumentieren und erfolgen mindestens in Textform (z. B. per E-Mail). Mündlich erteilte Weisungen wird Auftraggeber deshalb unverzüglich mindestens in Textform fixieren. Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Ohne Wissen von Auftraggeber werden keine Kopien und Duplikate erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer vertragsgemäßen Datenverarbeitung erforderlich sind, und Kopien oder Duplikate, die für die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

3.1.4. Auftragnehmer wird Auftraggeber umgehend informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Auftragnehmer ist berechtigt, entsprechende Weisungen so lange nicht durchzuführen, bis sie durch den Ansprechpartner beim Auftraggeber bestätigt oder geändert werden. Offensichtlich rechtswidrige Weisungen muss Auftragnehmer nicht durchführen.

3.2. **Datengeheimnis und Verpflichtung zur Vertraulichkeit**

Auftragnehmer stellt sicher, dass die Mitarbeiter, die auftragsgemäß auf personenbezogene Daten von Auftraggeber zugreifen können oder sonst Kenntnis von Daten von Auftraggeber erlangen können, zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und über die sich aus dieser AV-Vereinbarung ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt wurden. Sonstige Empfänger – insbesondere Unterauftragnehmer – die auftragsgemäß auf personenbezogene Daten von Auftraggeber zugreifen können, sind entsprechend zur Vertraulichkeit zu verpflichten. Auftragnehmer stellt sicher, dass die Personen, die Zugang zu den Daten von Auftraggeber haben, die Daten nur im Einklang der Weisungen von Auftraggeber verarbeiten. Hiervon ausgenommen sind Verarbeitungen, zu denen diese Personen gesetzlich verpflichtet sind.

3.3. **Technische und organisatorische Maßnahmen**

3.3.1. Auftragnehmer verpflichtet sich, nach den Maßgaben des Art. 32 DSGVO angemessene technische und organisatorische Maßnahmen zum Schutz der Daten vorzuhalten. Die aktuell zur Verfügung gestellten technischen und organisatorischen Maßnahmen sind in **Anlage 2** beschriebenen. Auftragnehmer legt auf schriftliche Anforderung von Auftraggeber die näheren Umstände der Festlegung offen, soweit hierdurch keine vorrangigen Interessen, insbesondere Geheimhaltungsinteressen, von Auftragnehmer betroffen sind.

3.3.2. Auftraggeber ist verpflichtet, Auftragnehmer vor Vertragsschluss und danach dauerhaft während der gesamten Laufzeit dieser AV-Vereinbarung rechtzeitig alle erforderlichen Informationen zu übermitteln, die Auftragnehmer für eine Bewertung der technischen und organisatorischen Maßnahmen nach Maßgabe des Art. 32 DSGVO benötigt. Auftraggeber weist unverzüglich und gesondert darauf hin, wenn besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet werden sollen (also Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung) oder sich aus anderen Gründen Besonderheiten bei der Beurteilung des Verarbeitungsrisikos ergeben. Dies gilt insbesondere für eine erhöhte

Eintrittswahrscheinlichkeit oder Schwere des Risikos für die Rechte und Freiheiten der Betroffenen.

3.3.3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei wird Auftragnehmer das angemessene Schutzniveau nicht unterschreiten. Wesentliche Änderungen sind zu dokumentieren.

4. **Einschaltung von Unterauftragnehmern**

4.1. Auftragnehmer wird nur Unterauftragnehmer einschalten, die er sorgfältig ausgewählt, geprüft und entsprechend Ziff. 3.2. verpflichtet hat. Auftraggeber erteilt seine allgemeine Zustimmung zur Einschaltung von Unterauftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten. Auftragnehmer informiert Auftraggeber über jede beabsichtigte Einschaltung eines Unterauftragnehmers. Auftraggeber hat die Möglichkeit zum Widerspruch innerhalb von 30 Tagen ab dem Zeitpunkt, zu dem der Ansprechpartner bei Auftraggeber von der beabsichtigten Einbindung durch Auftragnehmer in Kenntnis gesetzt wird. Bei Widerspruch gegen die Einbindung des Unterauftragnehmers werden Auftraggeber und Auftragnehmer versuchen, eine einvernehmliche Lösung zu finden. Wird keine einvernehmliche Lösung gefunden und ist die fortgesetzte Datenverarbeitung durch Auftragnehmer ohne die Einbindung des neuen Unterauftragnehmers unmöglich oder objektiv unzumutbar, kann Auftragnehmer diese AV-Vereinbarung und den korrespondierenden Leistungsvertrag aus wichtigem Grund kündigen. [Die eingesetzten Unterauftragnehmer sind in **Anlage 1** aufgeführt.]

4.2. Auftragnehmer wird durch vertragliche Vereinbarungen mit dem jeweiligen Unterauftragnehmer sicherstellen, dass die dem Unterauftragnehmer auferlegten Datenschutzpflichten in den wesentlichen Punkten denen von Auftragnehmer aus dieser AV-Vereinbarung entsprechen. Dies schließt angemessene Kontroll- und Überprüfungsrechte von Auftragnehmer und Auftraggeber ein, damit sichergestellt ist, dass die technischen und organisatorischen Maßnahmen entsprechend dieser AV-Vereinbarung umgesetzt werden. Auftraggeber hat das Recht, von Auftragnehmer auf Anforderung in Textform Auskunft über den wesentlichen Vertragsinhalt des Unterauftragsverhältnisses und des festgeschriebenen Pflichtenkatalogs zu erhalten, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen.

4.3. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die zur allgemein anerkannten und üblichen Betriebsorganisation gehören oder rein technischer Natur sind und deren Einsatz für Auftraggeber vorhersehbar sind (z. B.

Telekommunikationsleistungen, Reinigungskräfte, etc.), auch wenn die Kenntnisnahme personenbezogener Daten im Einzelfall nicht ausgeschlossen werden kann. Auftragnehmer ist gleichermaßen verpflichtet, angemessene und zumutbare Maßnahmen zur Gewährleistung des Schutzes und der Sicherheit der personenbezogenen Daten von Auftraggeber zu treffen.

5. **Mitwirkung bei Beantwortung der Betroffenenrechte (Berichtigung, Sperrung und Löschung von Daten)**

5.1. Die Wahrung der Betroffenenrechte gemäß Art. 12 - 22 DSGVO ist alleinige Verantwortung von Auftraggeber. Wenn sich ein Betroffener unmittelbar an Auftragnehmer wendet, um eine Berichtigung oder Löschung seiner Daten zu erwirken oder gegenüber Auftragnehmer der Datenverarbeitung widerspricht oder in Fällen von Profiling seinen eigenen Standpunkt mitteilt, wird Auftragnehmer dieses Ersuchen unverzüglich an Auftraggeber weiterleiten. Die Entscheidung, wie mit diesem Ersuchen umgegangen werden soll, wird Auftraggeber treffen. Auftragnehmer wird nur nach Weisung von Auftraggeber die Daten, die im Auftrag verarbeitet werden, berichtigen, löschen oder sperren. Dies gilt nicht bei entsprechender gesetzlicher Verpflichtung und im Falle von Ziff. 7.2. Auskünfte an den Betroffenen oder an Dritte wird Auftragnehmer nur nach vorheriger Zustimmung durch Auftraggeber erteilen.

5.2. Auftragnehmer wird Auftraggeber unter Berücksichtigung der Art der Verarbeitung sowie nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

5.3. Auftragnehmer wird personenbezogene Daten an Auftraggeber in dem Format herausgeben, wie sie Auftragnehmer von Auftraggeber zur Verarbeitung übermittelt wurden. Die Herausgabe in einem sonstigen strukturierten, gängigen und maschinenlesbaren Format ist nicht von Auftragnehmer zu leisten. Auch die Herausgabe direkt an den Betroffenen oder einen von diesem bestimmten weiteren Verantwortlichen wird Auftragnehmer nur aufgrund einer ausdrücklichen Weisung vornehmen und ausschließlich, wenn Auftraggeber die hierbei entstehenden zusätzlichen Kosten trägt.

6. **Unterstützung bei Einhaltung der Mitteilungspflichten bei Verstößen**

6.1. Auftragnehmer wird unverzüglich Auftraggeber benachrichtigen, wenn Auftragnehmer von einer Verletzung des Schutzes personenbezogener Daten erfährt. Der Hinweis enthält eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten und, soweit wie möglich, Angabe zu den Kategorien dieser personenbezogenen Daten und der ungefähren Zahl der betroffenen Personen. Es ist die alleinige Verantwortung von Auftraggeber, dass aus dieser Verletzung folgende Risiko zu bewerten. Auftragnehmer wirkt hieran durch die Meldung der Verletzung und die Bereitstellung der vorgenannten Informationen mit.

6.2. Auftragnehmer unterstützt Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikel 32 bis 36 DSGVO genannten Pflichten.

6.3. Wenn Empfehlungen der Aufsichtsbehörde gemäß Art. 36 Abs. 2 DSGVO Grundlage der Verarbeitung nach dieser AV-Vereinbarung werden sollen, so bestätigt dies der Auftraggeber ausdrücklich und schriftlich. Dies gilt insbesondere auch für Empfehlungen, die von der Aufsichtsbehörde direkt gegenüber Auftragnehmer gemacht werden. Auftragnehmer informiert Auftraggeber über solche Auftragnehmer unmittelbar mitgeteilte Empfehlungen und Fristverlängerungen der Aufsichtsbehörde gemäß Art. 36 Abs. 2 DSGVO. Auftragnehmer ist nur dazu verpflichtet, zusätzliche zu denen im Einklang mit Ziffer 3.3 getroffenen technischen und organisatorischen Maßnahmen umzusetzen, wenn Auftraggeber die hierdurch entstehenden zusätzlichen Kosten übernimmt.

6.4. Auftragnehmer informiert Auftraggeber über sonstige Beanstandungen, Anfragen oder Ersuchen hinsichtlich der Datenverarbeitung seitens Aufsichtsbehörden oder Betroffener, insbesondere über Kontrollhandlungen, Ermittlungen oder sonstige Maßnahmen von Aufsichtsbehörden, sofern geltendes Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

6.5. Auftragnehmer wird Auftraggeber alle erforderlichen Auskünfte erteilen. Dies betrifft auch Informationen zur Abwehr von Ansprüchen Dritter oder im Hinblick auf Anforderungen von Aufsichtsbehörden.

7. **Herausgabe und Löschung von Daten**

7.1. Auftraggeber kann jederzeit während der Laufzeit dieses Vertrages die Herausgabe oder Löschung seiner überlassenen bzw. in seinem Auftrag gespeicherten Datenbestände verlangen.

Mit Ende der jeweiligen Verarbeitungsleistung wird Auftragnehmer die Daten nach den nachfolgenden Ziffern herausgeben. Auftraggeber teilt Auftragnehmer rechtzeitig mit, wenn Daten für die auftragsgemäße Verarbeitung nicht weiter benötigt werden. Mit Ende des jeweiligen Leistungsvertrages ist die Verarbeitungsleistung in jedem Fall insgesamt abgeschlossen.

7.2. Auftragnehmer wird die Datenbestände für einen Zeitraum von 30 Tagen nach Ende der Auftragsverarbeitungsvereinbarung aufbewahren. Auftraggeber ist berechtigt, jederzeit bis zum Ablauf dieser Frist die Herausgabe oder Löschung der gespeicherten Daten zu verlangen.

7.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Auftragnehmer kann sie zur Entlastung bei Vertragsende Auftraggeber übergeben.

8. **Informations- und Kontrollmitwirkungspflichten**

8.1. Auftragnehmer wird bei Bedarf, nach angemessener Vorankündigung und entsprechenden Vertraulichkeitsvereinbarungen bei Bewertungen, Audits oder anderen Schritten zusammenarbeiten, die dem Zweck dienen, zu prüfen, ob die Verarbeitungstätigkeit von Auftragnehmer im Einklang mit dieser AV-Vereinbarung und geltendem Recht erfolgt. Der Auftraggeber trägt alle Kosten für diese Prüfmaßnahmen und sie müssen in einer Weise erfolgen, die das Geschäft von Auftragnehmer möglichst wenig stören. Soweit gesetzlich zulässig, kann Auftragnehmer statt der Prüfmaßnahmen eine Zusammenfassung der Ergebnisse einer Prüfung durch Dritte oder von Zertifizierungsberichten zur Verfügung stellen, die nachweisen, dass die Vorgaben der AV-Vereinbarung eingehalten werden. Solche Ergebnisse und/oder die Ergebnisse solcher Bewertungen, Prüfungen oder anderer Schritte sind vertrauliche Informationen von Auftragnehmer.

8.2. Auftragnehmer wird Auftraggeber auf begründete Anfrage, höchstens einmal pro Jahr, die Datenschutz- und Sicherheitsrichtlinien von Auftragnehmer und andere Informationen zur Verfügung stellen, die erforderlich sind, um nachzuweisen, dass die in dieser AV-Vereinbarung festgelegten Verpflichtungen eingehalten werden.

9. **Internationale Datentransfers**

Auftragnehmer stellt vor einem internationalen Datentransfer sicher, dass die gesetzlichen Anforderungen erfüllt sind, insbesondere, wenn ein internationaler Datentransfer in ein Drittland erfolgt, in dem das Datenschutzniveau unterhalb des Schutzniveaus innerhalb der Europäischen

Union entspricht. Dazu implementiert Auftragnehmer Schutzmechanismen. Zu diesen Schutzmechanismen können die von der EU-Kommission am 4. Juni 2021 angenommenen Standardvertragsklauseln (in der jeweils geänderten, aktualisierten oder ersetzten Fassung) („EU-SCCs“) oder ein von der Europäischen Kommission gemäß Artikel 45 DSGVO erlassener Angemessenheitsbeschluss gehören. Wenn Auftraggeber selbst in einem unsicheren Drittland ansässig ist (etwa den Vereinigten Staaten von Amerika), wird diese AV-Vereinbarung durch die EU-SCCs ergänzt, welche integraler Bestandteil dieser AV-Vereinbarung werden. Für den Datenrücktransfer an Auftraggeber gilt Modul 4 der EU-SCCs.

10. **Datenschutzbeauftragter**

Auftragnehmer hat aufgrund der gesetzlichen Vorgaben einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit ordnungsgemäß ausüben kann. Diese Funktion wird durch den folgenden Datenschutzbeauftragten wahrgenommen: Paul Matthews (pm@dna-network.de)

11. **Haftung**

11.1. Auftragnehmer haftet gegenüber Auftraggeber im Rahmen des Art. 82 Abs. 2 S. 2 DSGVO und nur dann, wenn Auftragnehmer schuldhaft eine ihn durch die DSGVO auferlegte Pflicht verletzt oder schuldhaft eine von Auftraggeber rechtmäßig erteilte Anweisung nicht beachtet oder gegen diese handelt.

11.2. Eine Haftung von Auftragnehmer ist ausgeschlossen, soweit die Pflichtverletzung alleine durch Auftraggeber verschuldet wurde. Insbesondere haftet Auftragnehmer gegenüber Auftraggeber nicht in Fällen, in denen die mit Auftraggeber abgestimmten technischen und organisatorischen Maßnahmen von Auftragnehmer deshalb nicht den Anforderungen nach Art. 32 DSGVO entsprechen, weil Auftraggeber seinen Informationspflichten nach 3.3.1. nicht oder nicht rechtzeitig nachkommt.

11.3. Auftragnehmer haftet für ein Verschulden seiner Unterauftragnehmer wie für eigenes Verschulden

11.4. Soweit eine Haftung von Auftragnehmer nach den vorstehenden Ziffern ganz oder teilweise ausgeschlossen ist, stellt Auftraggeber Auftragnehmer von allen Ansprüchen frei, die Dritte wegen der Datenverarbeitung im Auftrag von Auftraggeber gegen Auftragnehmer erheben. Das Gleiche gilt, soweit eine Inanspruchnahme durch Dritte den auf Auftragnehmer entfallenden Verschuldensanteil summenmäßig übersteigt. Auftraggeber ist verpflichtet, Auftragnehmer in

angemessener Weise bei der Verteidigung gegenüber den von Dritten erhobenen Ansprüchen zu unterstützen und alle geeigneten Beweismittel Auftragnehmer zugänglich zu machen.

12. **Allgemeine Bestimmungen**

12.1. Die Höhe der gesonderten Vergütungsansprüche für erhöhte Aufwände nach dieser Vereinbarung ergibt sich aus der Preisliste von Auftragnehmer.

12.2. Die Laufzeit dieser AV-Vereinbarung ist grundsätzlich zeitlich unbeschränkt. Mit dem Ende der Leistungsbeziehung zwischen Auftraggeber und Auftragnehmer erlischt auch diese AV-Vereinbarung automatisch.

12.3. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

12.4. Für alle Streitigkeiten im Zusammenhang mit dieser AV-Vereinbarung wird der Sitz von Auftragnehmer als ausschließlicher Gerichtsstand vereinbart, soweit Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Anlage 1: Auftragsspezifische Konkretisierung von Art und Umfang der Auftragsverarbeitung
Anlage 2: Technische und organisatorische Maßnahmen

Anlange 1: Spezifikation von Art und Umfang der Datenverarbeitung

Lfd. Anzah-ler	Zweck der Verarbeitung	Art der Verarbeitung	betroffene personenbezogene Daten	Kategorien von betroffenen Personen	Ort der Datenverarb eitung	Übermittlung von personenbezogenen Daten an Unterauftragsverarbeiter
1.	Digitale Verwaltung von Coaching-Sessions	Speichern, Lesen, Schreiben, Löschen, Bearbeiten	Name, Datum der Coaching-Session, ggf. ergänzende Kommentare des Auftraggebers Vollständiger Inhalt der Coaching-Session	Klienten des Auftraggebers	EU (Irland)	Salesforce Heroku (Webseite Hosting der Software, Datenbank via Heroku Postgres).
2.	Upload aufgezeichneter Coaching-Sessions in Form von Audiodateien	Speichern, Lesen, Schreiben, Löschen, Bearbeiten	Vollständiger Inhalt der Coaching-Session	Klienten des Auftraggebers	EU (Frankfurt, Deutschland)	Amazon Web Services (Vorübergehende Speicherung der Audio-Uploads)
3.	Transkripton der hochgeladenen Audiodateien	Speichern, Lesen, Schreiben, Löschen, Bearbeiten	Vollständiger Inhalt der Coaching-Session	Klienten des Auftraggebers	EU und USA	AssemblyAI (KI-gestützte Software zur Transkription)
4.	Analyse der Transkriptionen	Speichern, Lesen, Schreiben, Löschen, Bearbeiten	Vollständiger Inhalt der Coaching-Session	Klienten des Auftraggebers	EU und USA	Anthropic, PBC (Claude zur Durchführung der Analysen für Nutzer mit US-Datenresidenz)
5.	Analyse der Transkriptionen	Speichern, Lesen, Schreiben, Löschen, Bearbeiten	Vollständiger Inhalt der Coaching-Session	Klienten des Auftraggebers	EU	Mistral AI SAS (Mistral-Modelle zur Durchführung der Analysen für Nutzer mit EU-Datenresidenz)

Unter-Unterauftragsverarbeiter von Unterauftragsverarbeitern:

Unterauftragsverarbeiter	Unter-Unterauftragsverarbeiter	Zweck
Heroku Salesforce	AWS	Wie o.g. Salesforce Heroku (vgl. Ziff. 1)

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers

1. VERTRAULICHKEIT

1.1. Physische Zugangskontrolle

Technische oder organisatorische Maßnahmen zur Zugriffskontrolle, insbesondere auch zur Legitimation der Berechtigten, die sicherstellen, dass Unbefugte keinen Zugriff auf die Datenverarbeitungssysteme haben, mit denen personenbezogene Daten verarbeitet werden:

1.1.1. Telefone, Datenverarbeitungssysteme und Computer befinden sich in einem geschlossenen Bereich mit beschränktem Zugang;

1.2. System- und Datenzugang und Zugangskontrolle

Technische (Passwort/Passwortschutz) und organisatorische (Benutzerstammbuch) Maßnahmen zur Identifizierung und Authentifizierung der Benutzer, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren nutzen:

1.2.1. Richtlinien, die die Aufbewahrung von Sicherungskopien regeln.
1.2.2. (technisch) - Authentifizierung der Nutzer durch Passwort/PIN (Mindestlänge, Verwendung von Sonderzeichen usw.)
1.2.3. (Technisch) - Authentifizierung durch biometrische Daten
1.2.4. (technisch) - Authentifizierung über Chip/Schlüsselkarte oder mobiles Gerät
1.2.5. (Technisch) - Einsatz von Antiviren-Software
1.2.6. (Technisch) - Verwaltung mobiler Geräte
1.2.7. (technisch) - Multi-Faktor-Authentifizierung (intern/extern)
1.2.8. (Technisch) - Blockieren externer Schnittstellen (z.B. USB-Ports)
1.2.9. (Technisch) - Protokollierung der Datenvernichtung
1.2.10. (Organisatorisches) - Weitergabe von Daten nur an berechtigte Personen;
1.2.11. (Organisatorisch) - Benutzerverwaltung (nur autorisierte/berechtigte Personen erhalten Basiszugang)
1.2.12. (Organisatorisch) - Passwortvergabe/Passwortregeln (Länge, Änderung, etc.) -
1.2.13. (Organisatorisches) - Richtlinien für Mitarbeiter sowie Schulungen zu einzelnen Arbeitsabläufen und Zugriffsberechtigungen auf personenbezogene Daten;
1.2.14. (Organisatorisch) - Reduzierung der Zahl der Administratoren auf das notwendige "Minimum".
1.2.15. (Organisatorisch) - Entwicklung eines Berechtigungskonzepts und Freigabe der Daten nur für berechtigte Personen
1.2.16. (Organisatorische) - Wirksame und angemessene disziplinarische Maßnahmen gegen Personen, die unbefugt auf personenbezogene Daten zugreifen.

1.3. Kontrolle der Übertragung

Maßnahmen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übermittlung oder während des Transports oder der Speicherung auf Datenträgern (manuell oder elektronisch) nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass es möglich ist, (im Nachhinein) zu überprüfen und festzustellen, an welche Stellen eine Übermittlung personenbezogener Daten stattgefunden hat:

1.3.1. (Technisch) - Verwendung von sicheren Verbindungen (z.B. verschlüsselt/VPN/TLS).
1.3.2. (Organisatorisches) - Dokumentation der Datenempfänger und des Zeitpunkts der geplanten Übertragungen zur Nutzung oder der vereinbarten Löschungsfristen.
1.3.3. (Organisatorische) - Übermittlung von Daten in anonymisierter oder pseudonymisierter Form.
1.3.4. (Organisatorisches) - Liste der Verfahren
1.3.5. (Organisatorische) - Maßnahmen aufzeichnen

1.4. Pseudonymisierung

Maßnahmen, bei denen der Name oder andere Identifizierungsmerkmale durch eine Markierung ersetzt werden, um die Identifizierung der betroffenen Person auszuschließen oder erheblich zu erschweren:

1.4.1. (Organisatorische) - Strenge Zugangsbeschränkungen für Informationen, die den Betroffenen selbst erkennen lassen.

1.5. Verschlüsselung

1.5.1. (Technisch) - Verschlüsselung von (mobilen) Datenträgern/Wechseldatenträgern
1.5.2. (technisch) - Zugriff nur über gesicherte/verschlüsselte Verbindung möglich
1.5.3. (technisch) - Verschlüsselung von Datenträgern (nach Industriestandard)
1.5.4. (Technisch) - E-Mail-Verschlüsselung
1.5.5. (Technisch) - Verschlüsselte Speicherung gemäß den geltenden Industriestandards.

2. INTEGRITÄT

2.1. Eingabe / Eingabekontrolle

Maßnahmen, die gewährleisten, dass im Nachhinein überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder gelöscht wurden:

2.1.1. Maßnahmen zum Schutz vor unbefugter Veränderung und/oder Löschung der gespeicherten Daten;
2.1.2. (Technisch) - Aufzeichnung der Eingabe, Änderung und Löschung von Daten.
2.1.3. (Technisch) - Benutzeridentifikation gemäß Zugangskontrolle
2.1.4. (Technisch) - Protokollierung des Zugriffs auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten.
2.1.5. (Organisatorisch) - Erstellung einer Übersicht über Anwendungen, in denen Daten eingegeben, geändert und gelöscht wurden.
2.1.6. (Organisatorische) - Transparenz der Dateneingabe, -änderung und -löschung durch individuelle Benutzernamen (keine Benutzergruppen)
2.1.7. (Organisatorische) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts

2.2. Integritätskontrolle (Erkennung von Integritätsverletzungen)

2.2.1. (Technische) - Regelmäßige Überprüfung der Integrität der Daten.
2.2.2. (Technisch) - Erkennung von Integritätsverletzungen in Echtzeit.

3. VERFÜGBARKEIT UND ZUVERLÄSSIGKEIT

3.1. Verfügbarkeitskontrolle

Datensicherheitsmaßnahmen (physisch/logisch), die gewährleisten, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

3.1.1. (Technische) - Vorschriften zum Verbot der Speicherung personenbezogener Daten auf lokalen Datenträgern.
3.1.2. (technisch) - Redundanz der Infrastruktur (z. B. Lastausgleich, RAID usw.)
3.1.3. (Technisch) - Antiviruskonzept/Malwareschutz/IDS/IPS
3.1.4. (technisch/organisatorisch) - Regelmäßige Datensicherung nach dem Backup- und Recovery-Konzept
3.1.5. (Organisatorisches) - Wirksamer Notfallplan
3.1.6. (Organisatorisch) - Proaktive Überwachung der Ressourcen auf Engpässe oder mögliche Ausfälle.

3.2. Kontrolle der Tragfähigkeit

Maßnahmen, die sicherstellen, dass Datenverarbeitungssysteme auch in Stresssituationen störungsfrei funktionieren:

3.2.1. (Technisch) - Kontinuierliche Leistungsüberwachung und proaktive Behebung von Engpässen.
3.2.2. (Organisatorische) - Leistungstests während der Entwicklung und bei Änderungen.

3.3. Kontrolle der Rückgewinnbarkeit

3.3.1. (Organisatorisch) - Regelmäßige Überprüfung der Wiederherstellung von Backups.

4. PROZESSKONTROLLE UND EVALUIERUNG DES SICHERHEITSKONZEPTS

4.1. Vertrags-/Auftragskontrolle

4.1.1. Zugangskontrollen wie unter 1.2 beschrieben
4.1.2. (Organisatorische) - Regelmäßige Validierung der Zugangsrechte
4.1.3. (Organisatorisches) - Klare schriftliche Anweisungen an den Auftragsverarbeiter über den Umfang der Verarbeitung personenbezogener Daten.
4.1.4. (Organisatorisches) - Sicherstellung der Vernichtung von Daten nach Vertragsende.

4.1.5. (Organisatorisch) - Sicherstellung der Einhaltung des Datenschutzes durch das Personal des Auftragsverarbeiters.
4.1.6. (Organisatorische) - Vorabkontrolle der vom Verarbeiter getroffenen Sicherheitsmaßnahmen und der entsprechenden Dokumentation.

4.2. Kontrolle der Abtrennung

Maßnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können.

4.2.1. (Technisch) - Module in der Datenbank des Auftragnehmers unterscheiden die verschiedenen Verwendungszwecke der Daten, z. B. Unterscheidung nach Funktionalität und Funktion;
4.2.2. (Technisch) - Schnittstellen, Stapelverarbeitung und Berichte werden nur für bestimmte Zwecke und Funktionen konfiguriert, so dass die für bestimmte Zwecke gesammelten Daten getrennt verarbeitet werden können.
4.2.3. (technisch) - Physikalisch getrennte Speicherung auf separaten Systemen oder Datenträgern.
4.2.4. (Technisch) - Trennung zwischen Produktiv- und Testsystem
4.2.5. (Technische) - Sicherheitsmaßnahmen, die sicherstellen, dass nur autorisierte Benutzer auf die Daten zugreifen können.
4.2.6. (Technische) - Sicherheitsmaßnahmen, die sicherstellen, dass nur autorisierte Benutzer auf die Daten zugreifen können.
4.2.7. (Technisch) - Logische Client-Trennung (Software-Seite)
4.2.8. (Organisatorisches) - Entwicklung eines Berechtigungskonzeptes
4.2.9. (Organisatorisch) - Bereitstellung von Datensätzen mit Zweckattributen/Datenfeldern.

4.3. Kontrolle der Aufbewahrung/Löschung

4.3.1. (Organisatorisch) - Beispielhafte Überprüfung von Löschungen oder Einstellungen.

4.4. Standardmäßiger Schutz

4.4.1. (Organisatorisch) - Überprüfung der Anforderungen im Hinblick auf die Umsetzung.
4.4.2. (Organisatorisch) - Systemeinstellungen prüfen

4.5. Datenschutzmanagement / Wirksamkeitskontrollen / Zertifikate

4.5.1. (Organisatorisch) - Regelmäßige Bereitstellung von Sicherheits-/Datenschutzzertifikaten.
4.5.2. (Organisatorische) - Regelmäßige Überprüfung des Lieferanten.