Vertrag zur Auftragsverarbeitung

zwischen

dem Nutzer, der die Allgemeinen Geschäftsbedingungen des Auftragnehmers akzeptiert und den Vertrag über die Plattform „Voicely" abgeschlossen hat (hier bezeichnet als „Auftraggeber")

und

RelationFlow Ltd.

Anthypolochagou Georgiou M. Savva 26, Office 1-2

8201 Paphos, Zypern (CY)

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer")

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Dieser Vertrag gilt ausschließlich für Geschäftskunden im Sinne der Allgemeinen Geschäftsbedingungen des Auftragnehmers.

Voicely stellt zwei Verarbeitungsebenen zur Verfügung:

(a) Cloudbasierte Verarbeitungsebene (Cloud): Sprachdaten und die daraus erzeugten Transkriptionen werden an die in Anlage 4 genannten Unterauftragsverarbeiter übermittelt und verarbeitet. Für diese Ebene gilt der vorliegende Vertrag vollumfänglich.

(b) Lokale Verarbeitungsebene (Local): Sprachdaten und Transkriptionen verbleiben auf dem Endgerät des Auftraggebers und werden weder an den Auftragnehmer noch an Dritte übermittelt. Insoweit findet keine Auftragsverarbeitung statt. Klarstellung: Konto-, Einstellungs- und Synchronisationsdaten (insbesondere benutzerdefiniertes Wörterbuch, Textbausteine und Tonalitäten) sowie Authentifizierungsdaten werden auch bei Nutzung der lokalen Verarbeitungsebene weiterhin cloudseitig verarbeitet. Für diese Daten gilt der vorliegende Vertrag fort.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer

Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrische Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für den Auftraggeber ist die für den Sitz des Auftraggebers zuständige Datenschutzaufsichtsbehörde.

(2) Der Auftragnehmer hat seinen Sitz in der Republik Zypern. Zuständige Aufsichtsbehörde für den Auftragnehmer ist:

Office of the Commissioner for Personal Data Protection

(Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

Iasonos 1, 1082 Nicosia, Zypern

commissioner@dataprotection.gov.cy

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber folgende Leistungen: Bereitstellung der Voicely-Anwendung zur KI-gestützten Umwandlung von Sprache in Text, die Verarbeitung von Sprachdaten über die cloudbasierte Verarbeitungsebene, sowie etwaige zusätzliche Funktionen gemäß der Leistungsbeschreibung auf der Website. Dies geschieht auf Grundlage des über den Self-Service-Prozess (Download und Registrierung) abgeschlossenen Vertrags auf Basis der Allgemeinen Geschäftsbedingungen des Auftragnehmers („Hauptvertrag"). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 5. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

(3) Der Auftraggeber bestimmt allein durch seine Nutzung der Anwendung, welche Inhalte er diktiert und damit verarbeiten lässt. Die Diktatinhalte können daher jede Kategorie personenbezogener Daten enthalten, einschließlich besonderer Kategorien personenbezogener Daten im Sinne des § 1 Abs. 4 dieses Vertrages sowie personenbezogener Daten Dritter. Der Auftraggeber ist dafür verantwortlich, dass für diese Verarbeitung eine Rechtsgrundlage besteht und die Betroffenen ordnungsgemäß informiert werden.

(4) Berufs- und Amtsgeheimnisse (§ 203 StGB): Inhalte, die einem Berufs- oder Amtsgeheimnis im Sinne des § 203 StGB unterliegen — insbesondere Patienten-, Mandanten- und Klientendaten — dürfen ausschließlich über die lokale Verarbeitungsebene (Local) verarbeitet werden. Die cloudbasierte Verarbeitungsebene ist für solche Inhalte nicht bestimmungsgemäß.

(5) Der Auftraggeber stellt sicher, dass seine autorisierten Nutzer für Inhalte nach Absatz 4 ausschließlich die lokale Verarbeitungsebene verwenden. Er stellt ferner sicher, dass keine geheimnisgeschützten Angaben (insbesondere Namen von Patienten, Mandanten oder Klienten) in das benutzerdefinierte Wörterbuch, in Textbausteine oder in Tonalitäten aufgenommen werden. Klarstellung: Diese Einstellungsdaten werden auch bei aktivierter lokaler Verarbeitungsebene mit den Servern des Auftragnehmers synchronisiert und verlassen insoweit das Endgerät.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der Datensicherheit. Die in Anlage 3 beschriebenen Maßnahmen umfassen sowohl eigene Maßnahmen des Auftragnehmers als auch Maßnahmen der eingesetzten Unterauftragsverarbeiter. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als Datenschutzbeauftragter bestellt:

NUM3RUS GmbH

Fernando Fernandez

Carmenstr. 9

40549 Düsseldorf

datenschutz@kiberatung.de

Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegt.

(5) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des

Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Unterauftragsverarbeitern

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in Anlage 4 aufgeführten Unterauftragsverarbeiter einzusetzen. Anlage 4 führt sämtliche Unterauftragsverarbeiter auf, einschließlich der KI-Dienste, die für die Sprachtranskription und die KI-gestützte Textverarbeitung eingesetzt werden.

(2) Klarstellung zur Rolle der KI-Dienste: Der Auftragnehmer wählt die eingesetzten KI-Dienste aus, hält die zugehörigen Zugangsschlüssel und übermittelt die Sprach- und Textdaten selbst an diese Dienste. Der Auftraggeber unterhält keine eigene Vertragsbeziehung zu diesen Diensten. Die KI-Dienste sind daher Unterauftragsverarbeiter im Sinne des Art. 28 Abs. 2 und 4 DS-GVO und in Anlage 4 aufgeführt.

(3) Der Auftragnehmer ist befugt, weitere Unterauftragsverhältnisse zu begründen. Er setzt den Auftraggeber hiervon vorab in Textform in Kenntnis. Der Auftraggeber hat die Möglichkeit, innerhalb von 14 Tagen nach Zugang der Mitteilung Einspruch zu erheben. Im Falle eines berechtigten Einspruchs steht dem Auftraggeber ein Sonderkündigungsrecht hinsichtlich des Hauptvertrags zu.

(4) Der Auftragnehmer ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Er hat sie entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch gegenüber den Unterauftragsverarbeitern wahrnehmen kann. Sofern eine Einbeziehung von Unterauftragsverarbeitern in einem Drittland erfolgt, hat der Auftragnehmer sicherzustellen, dass ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Angemessenheitsbeschluss, EU-Standardvertragsklauseln oder eine Zertifizierung nach dem EU-US Data Privacy Framework). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen nachweisen.

(5) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Die Anwendung stellt hierfür insbesondere folgende Funktionen bereit: Jeder Nutzer kann seine vollständige Diktathistorie sowie sein Wörterbuch, seine Textbausteine und seine Tonalitäten selbst als CSV-Datei exportieren (Art. 20 DS-GVO). Jeder Nutzer kann sein Nutzerkonto und die zugehörigen Daten selbst in der Anwendung löschen (Art. 17 DS-GVO).

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen.

(2) Die Löschung aus den Produktivsystemen des Auftragnehmers erfolgt innerhalb von 30 Tagen nach Beendigung des Hauptvertrags bzw. nach Zugang eines entsprechenden Verlangens des Auftraggebers.

(3) Datensicherungen: Der Hosting-Dienstleister des Auftragnehmers erstellt tägliche Sicherungen der Datenbestände. Eine gezielte Einzellöschung aus bereits erstellten Datensicherungen ist technisch nicht möglich. Gelöschte Daten verbleiben daher bis zum Ablauf der Aufbewahrungsdauer der jeweiligen Datensicherung in dieser und werden anschließend durch deren Rotation überschrieben. Innerhalb dieses Zeitraums werden die Daten nicht mehr aktiv verarbeitet.

(4) Der Auftragnehmer bestätigt dem Auftraggeber die Löschung auf dessen Verlangen in Textform.

(5) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(6) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag werden nach der Schiedsgerichtsordnung der Deutschen Institution für Schiedsgerichtsbarkeit e.V. (DIS) unter Ausschluss des ordentlichen Rechtswegs endgültig entschieden. Das Schiedsgericht besteht aus einem Einzelschiedsrichter. Der Schiedsrichter soll über besondere Sachkunde im Bereich Informationstechnologie oder Künstliche Intelligenz verfügen. Schiedsort ist München.

Anlagen

Anlage 1 – Beschreibung der Datenkategorien

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 4 – Genehmigte Unterauftragsverarbeiter

Anlage 5 – Weisungsberechtigte Personen

Anlage 1 – Beschreibung der Datenkategorien

Grundsatz: Der Auftraggeber bestimmt durch seine Nutzung der Anwendung allein, welche Inhalte er diktiert. Die Diktatinhalte können daher jede Kategorie personenbezogener Daten enthalten, einschließlich besonderer Kategorien personenbezogener Daten nach Art. 9 DS-GVO (insbesondere Gesundheitsdaten) sowie personenbezogener Daten Dritter.

Im Rahmen der Nutzung der cloudbasierten Verarbeitungsebene werden folgende Kategorien personenbezogener Daten verarbeitet:

1. Registrierungs- und Kontodaten: Name, E-Mail-Adresse, Profilbild, Team-Zugehörigkeit und Rolle.

2. Sprachdaten (Audioaufnahmen): Werden zur Transkription an den in Anlage 4 genannten Transkriptionsdienst übermittelt. Audiodaten werden weder auf dem Endgerät noch auf Servern des Auftragnehmers dauerhaft gespeichert. Zur Speicherung beim Transkriptionsdienst siehe Anlage 4 Ziffer 1.

3. Transkriptionen und KI-verarbeitete Texte: Werden verschlüsselt in der Diktathistorie des Nutzers gespeichert (siehe Anlage 3).

4. Kontextdaten der Zielanwendung: Name der zum Zeitpunkt des Diktats aktiven Anwendung sowie deren Fenstertitel. Diese Angaben werden zur Steuerung der Textformatierung an den in Anlage 4 genannten KI-Dienst für Textverarbeitung übermittelt und gemeinsam mit dem Diktat gespeichert. Hinweis: Fenstertitel können personenbezogene Daten Dritter enthalten (z. B. Betreffzeilen oder Namen in Anwendungsfenstern).

5. Benutzerdefiniertes Wörterbuch, Textbausteine und Tonalitäten: Werden zur Verbesserung der Erkennungsgenauigkeit teilweise an den Transkriptionsdienst und den KI-Dienst für Textverarbeitung übermittelt. Hinweis: Wörterbucheinträge können Namen enthalten.

6. Bildschirmfotos der aktiven Anwendung: Nur bei ausdrücklicher Aktivierung durch den Nutzer. Speicherung in einem privaten, zugriffsbeschränkten Speicherbereich. Hinweis: Bildschirmfotos können beliebige personenbezogene Daten Dritter abbilden.

7. Nutzungs- und Abrechnungsdaten: Wortanzahl, Audiodauer, Zeitstempel, Kostenkennzahlen.

8. Support- und Kommunikationsdaten: Inhalte von Support-Anfragen einschließlich der darin enthaltenen personenbezogenen Daten.

9. Telemetriedaten: Fehler- und Nutzungsdaten in pseudonymisierter Form (siehe Anlage 3 und Anlage 4).

Bei Nutzung der lokalen Verarbeitungsebene (Local) verbleiben Sprachdaten und Transkriptionen ausschließlich auf dem Endgerät des Auftraggebers. Die unter Ziffer 1, 5, 7 und 9 genannten Daten werden auch in diesem Modus cloudseitig verarbeitet.

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

– Mitarbeiter und sonstige autorisierte Nutzer des Auftraggebers

– Personen, deren Stimmen in den verarbeiteten Sprachaufnahmen enthalten sind

– Personen, auf die sich die Inhalte der Diktate beziehen (insbesondere Patienten, Mandanten, Kunden und Geschäftspartner des Auftraggebers)

– Personen, die in Fenstertiteln oder Bildschirmfotos erscheinen

– Personen, deren Namen im benutzerdefinierten Wörterbuch erfasst sind

– Kommunikationspartner im Rahmen von Support-Anfragen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle: Der Auftragnehmer betreibt keine eigenen Rechenzentren. Der physische Schutz erfolgt durch die in Anlage 4 genannten Infrastruktur-Dienstleister nach deren jeweiligen technischen und organisatorischen Maßnahmen.

Zugangskontrolle:

– Passwortrichtlinie für Nutzerkonten (Mindestlänge, Zeichenklassen)

– Zeitlich begrenzte Zugriffstoken mit automatischer Rotation

– Speicherung der Sitzungsdaten im Schlüsselbund des Betriebssystems

– Administrativer Zugang ausschließlich mit verpflichtender Zwei-Faktor-Authentifizierung (TOTP) und Backup-Codes; erneute Authentifizierung nach Ablauf des Gültigkeitsfensters

Zugriffskontrolle:

– Row-Level-Security auf allen Datenbanktabellen mit personenbezogenen Daten: Ein Nutzer kann ausschließlich auf die ihm bzw. seinem Konto zugeordneten Datensätze zugreifen

– Private, nicht öffentlich adressierbare Speicherbereiche für Bildschirmfotos und Profilbilder

– Berechtigungskonzept nach dem Need-to-Know-Prinzip für Mitarbeiter des Auftragnehmers

– Protokollierung administrativer Zugriffe

Trennungskontrolle: Mandantentrennung über kontobezogene Kennungen in Verbindung mit Row-Level-Security.

Pseudonymisierung:

– Fehlerdiagnose (Sentry): keine Übermittlung von Nutzeridentifikatoren im Klartext; automatische Entfernung von E-Mail-Adressen, Zugangstoken, Schlüsseln und Dateipfaden vor Übermittlung

– Produktanalyse (PostHog): serverseitige Ereignisse ausschließlich mit gehashten Nutzerkennungen; keine Sitzungsaufzeichnung

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle:

– Transportverschlüsselung (TLS/WSS) für sämtliche Verbindungen

– Zugangsschlüssel zu den KI-Diensten verlassen die Server des Auftragnehmers nicht; die Client-Anwendung erhält ausschließlich kurzlebige Einmal-Token

– Regionsbindung (technisch erzwungen, nicht nur organisatorisch):

· Die Anwendung führt eine Positivliste zulässiger Verbindungsziele (Content-Security-Policy). Verbindungen zu anderen als den dort genannten Zielen werden vom Programm blockiert.

· Für die Sprachtranskription ist ausschließlich der EU-Data-Residency-Endpoint des Dienstleisters zugelassen; dessen außereuropäische Endpunkte sind gesperrt.

· Für die Fehlerdiagnose ist ausschließlich der EU-Endpunkt des Dienstleisters zugelassen; der außereuropäische Endpunkt ist gesperrt.

· Der KI-Dienst für Textverarbeitung ist serverseitig auf die Region eu-north1, einen festen Host und eine geschlossene Liste zugelassener Modelle beschränkt; abweichende Regionen führen zum Abbruch der Verarbeitung (fail-closed).

– Keine Speicherung beim KI-Dienstleister: Bei jedem Transkriptions- und Textverarbeitungsvorgang werden Parameter gesetzt, die eine Speicherung der übermittelten Inhalte beim Dienstleister unterbinden

Verschlüsselung ruhender Daten:

– Diktate (Transkript und verarbeiteter Text) werden bereits auf dem Endgerät des Nutzers mit AES-256-GCM verschlüsselt, bevor sie in die Datenbank geschrieben werden

– Klarstellung: Es handelt sich um eine anwendungsseitige Feldverschlüsselung, nicht um eine Ende-zu-Ende- oder Zero-Knowledge-Verschlüsselung. Der Auftragnehmer kann die Inhalte technisch entschlüsseln.

– Keine Persistenz von Audiodaten: Sprachaufnahmen werden in den Systemen des Auftragnehmers zu keinem Zeitpunkt auf einen Datenträger geschrieben; zur Speicherung beim Transkriptionsdienst siehe Anlage 4 Ziffer 1

Integrität der Software:

– Signierte Anwendungspakete und signierte Aktualisierungen

– Prüfsummenverifikation aller nachgeladenen KI-Modelle

– Signaturprüfung eingehender Webhooks

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)

– Tägliche Sicherung der Datenbestände durch den Hosting-Dienstleister

– Begrenzung der Anfragerate pro Nutzer auf allen Transkriptions-, KI- und Abrechnungsschnittstellen zum Schutz vor Überlastung und Missbrauch

– Fehler- und Ausfallüberwachung mit Alarmierung

IV. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DS-GVO)

– Automatisierte Sicherheits- und Qualitätsprüfungen im Entwicklungsprozess

– Regelmäßige Überprüfung der Zugriffsberechtigungen

– Überprüfung der Datenschutz- und Sicherheitsmaßnahmen bei wesentlichen Produktänderungen

V. Maßnahmen der Unterauftragsverarbeiter

Ergänzend gelten die technischen und organisatorischen Maßnahmen der in Anlage 4 genannten Unterauftragsverarbeiter:

– Vercel: https://vercel.com/legal/dpa#schedule-2

– Supabase: https://supabase.com/downloads/docs/Supabase+DPA+250314.pdf (Schedule 1)

– Upstash: https://upstash.com/static/trust/security-measures.pdf

VI. Lokale Verarbeitungsebene (nicht Gegenstand der Auftragsverarbeitung)

Bei Nutzung der lokalen Verarbeitungsebene werden Diktate in einer verschlüsselten lokalen Datenbank (SQLCipher) auf dem Endgerät des Nutzers gespeichert; der Schlüssel wird im Schlüsselbund des Betriebssystems verwahrt.

Anlage 4 – Genehmigte Unterauftragsverarbeiter

Die nachfolgenden Unternehmen sind genehmigte Unterauftragsverarbeiter im Sinne des § 9:

1. ElevenLabs Inc.

Adresse: 1732 1st Ave #20667, New York, NY 10128, USA

Aufgabe: Sprachtranskription (Speech-to-Text)

Übermittelte Daten: Sprachaufnahmen (Audio), Sprachcode, Begriffe aus dem benutzerdefinierten Wörterbuch zur Verbesserung der Erkennungsgenauigkeit

Verarbeitungsort: EU (EU-Data-Residency-Endpoint)

Garantie: Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO; Verarbeitung über den EU-Data-Residency-Endpoint; für Support- und Missbrauchsprüfungen des Anbieters von außerhalb der Union Standardvertragsklauseln (SCC) sowie EU-US Data Privacy Framework. Speicherung beim Anbieter: Der Auftragnehmer fordert bei jedem Aufruf an, dass keine Protokolle angelegt werden; der Anbieter wendet dies nur im Rahmen seines Enterprise-Tarifs an. In der Echtzeit-Transkription führt der Anbieter daher ein eigenes Verarbeitungsprotokoll, das die übermittelte Aufnahme und den erkannten Text umfasst. Im Stapelbetrieb entfernt der Auftragnehmer das entstehende Transkript unmittelbar nach der Übertragung über die Löschschnittstelle des Anbieters.

DPA: https://elevenlabs.io/privacy

2. Deepgram, Inc.

Adresse: 1418 NW 53rd St, Seattle, WA 98107, USA

Aufgabe: Sprachtranskription (Speech-to-Text) — alternativer Dienst. Er wird vom Auftragnehmer eingesetzt, wenn der unter Ziffer 1 genannte primäre Transkriptionsdienst gestört oder nicht verfügbar ist.

Übermittelte Daten: Sprachaufnahmen (Audio), Sprachcode, Begriffe aus dem benutzerdefinierten Wörterbuch zur Verbesserung der Erkennungsgenauigkeit

Verarbeitungsort: EU (EU-Endpoint)

Garantie: Standardvertragsklauseln (SCC); Widerspruch gegen die Nutzung der Daten zu Modelltrainingszwecken ist aktiviert (Model Improvement Program Opt-out)

DPA: https://deepgram.com/dpa

3. Nebius B.V. (Nebius Token Factory)

Adresse: Schiphol Boulevard 165, 1118 BG Schiphol, Niederlande

Aufgabe: KI-gestützte Textverarbeitung (LLM)

Übermittelte Daten: Transkript, Name und Fenstertitel der aktiven Zielanwendung, Tonalitätsvorgaben, Kontext aus dem benutzerdefinierten Wörterbuch

Verarbeitungsort: EU (Region eu-north1, technisch erzwungen)

Garantie: Verarbeitung ausschließlich in der EU; Standardvertragsklauseln (SCC)

DPA: https://docs.tokenfactory.nebius.com/legal/dpa

4. Supabase Inc.

Adresse: 970 Toa Payoh North #07-04, Singapore 318992

Aufgabe: Datenbank, Authentifizierung, Serverfunktionen, Dateispeicher

Übermittelte Daten: sämtliche in Anlage 1 genannten Datenkategorien

Verarbeitungsort: EU (Frankfurt)

Garantie: Standardvertragsklauseln (SCC)

DPA: https://supabase.com/downloads/docs/Supabase+DPA+250314.pdf

5. Vercel Inc.

Adresse: 440 N Barranca Ave #4133, Covina, CA 91723, USA

Aufgabe: Hosting der Website und des Verwaltungsbereichs

Übermittelte Daten: IP-Adressen und Verbindungsmetadaten der Websitebesucher

Verarbeitungsort: EU (Frankfurt, fra1) / US

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

DPA: https://vercel.com/legal/dpa

6. Upstash Inc.

Adresse: 1000 N West Street, Suite 1200, Wilmington, DE 19801, USA

Aufgabe: Begrenzung der Anfragerate (Rate Limiting)

Übermittelte Daten: pseudonyme Nutzerkennung, Name des aufgerufenen Endpunkts; keine Inhaltsdaten

Verarbeitungsort: EU (AWS-Region eu-central-1, Frankfurt)

Garantie: Standardvertragsklauseln (SCC)

DPA: https://upstash.com/trust/dpa.pdf

7. Stripe Payments Europe, Ltd.

Adresse: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland

Aufgabe: Zahlungsabwicklung

Übermittelte Daten: Name, E-Mail-Adresse, Rechnungsadresse, Steuer-Identifikationsnummer, Zahlungsdaten

Verarbeitungsort: EU (Irland), Konzernmutter USA

Garantie: EU-US Data Privacy Framework

DPA: https://stripe.com/de/legal/dpa

8. Resend Inc.

Adresse: 2261 Market Street #4059, San Francisco, CA 94114, USA

Aufgabe: Versand transaktionaler E-Mails sowie Empfang und Verarbeitung eingehender Support-E-Mails

Übermittelte Daten: E-Mail-Adresse, Name, vollständiger Inhalt aus- und eingehender E-Mails

Verarbeitungsort:

– Versand: EU (Irland, eu-west-1) — alle Versanddomänen des Auftragnehmers sind auf diese Region konfiguriert

– Speicherung: USA. Der Anbieter speichert Kontodaten, E-Mail-Metadaten, Protokolldaten und API-Aufzeichnungen nach eigener Dokumentation unabhängig von der gewählten Versandregion in den Vereinigten Staaten.

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

DPA: https://resend.com/legal/dpa

9. Functional Software Inc. (Sentry)

Adresse: 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA

Aufgabe: Fehler- und Absturzüberwachung

Übermittelte Daten: technische Fehlermeldungen, Stapelüberwachungen, pseudonyme Nutzerkennung; keine Diktatinhalte

Verarbeitungsort: EU (EU-Ingest-Endpoint; die Anwendung lässt technisch keinen anderen Endpunkt zu)

Garantie: Standardvertragsklauseln (SCC)

DPA: https://sentry.io/legal/dpa/

10. PostHog Inc.

Adresse: 2261 Market Street #4008, San Francisco, CA 94114, USA

Aufgabe: Produkt- und Nutzungsanalyse

Übermittelte Daten: Ereignisdaten mit pseudonymer Nutzerkennung; keine Diktatinhalte

Verarbeitungsort: EU (EU-Endpoint)

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

DPA: https://posthog.com/dpa

11. GitHub, Inc. (Microsoft Corporation)

Adresse: 88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, USA

Aufgabe: Auslieferung der Anwendung und der Aktualisierungen; Überführung von Support-Anfragen in interne Fehlertickets

Übermittelte Daten: bei Downloads und Aktualisierungen ausschließlich IP-Adresse und Verbindungsmetadaten; bei der Überführung von Support-Anfragen zusätzlich Betreff und Inhalt der Support-Anfrage

Verarbeitungsort: USA

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

DPA: https://github.com/customer-terms/github-data-protection-agreement

---

Anlage 5 – Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers werden mit dem Abschluss des „Self Service"-Vertrags festgelegt. Ausschließlich die beim Abschluss hinterlegten Adressen sind weisungsberechtigt.

Der Weisungsempfänger beim Auftragnehmer ist erreichbar unter: support@voicely.de

---