# Auftragsverarbeitungsvertrag
# gemäß Art. 28 DSGVO (Datenschutz-Grundverordnung)

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

voize GmbH, vertreten durch Marcel Schmidberger, Dircksenstraße 47, 10178 Berlin
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## § 1 Vertragsgegenstand

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend Daten genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung.

Die Beauftragung durch den Auftraggeber wird durch einen oder mehrere Hauptverträge bestimmt. Dies können z.B. Dienstleistungsverträge oder beauftragte Angebote bzw. Leistungsbeschreibungen sein (nachstehend Hauptvertrag genannt).

Die konkreten Verarbeitungstätigkeiten der Auftragsverarbeitung im Zusammenhang mit dem Hauptvertrag, insbesondere die Art der Daten, der Zweck der Datenerhebung, Datenverarbeitung und -nutzung, sowie der Kreis der Betroffenen sind in Anlage 1 (Link der Anlage einfügen) beschrieben. Die Verarbeitungstätigkeiten richten sich nach der Nutzung durch den Verantwortlichen. Es gelten entsprechend der Nutzung die beschriebenen Module.

Der Auftragnehmer darf die Daten ausschließlich pseudonymisiert nutzen und diese zum Zweck der bedarfsgerechten Gestaltung, Weiterentwicklung und Optimierung verarbeiten. Die Parteien stimmen darin überein, dass pseudonymisierte Daten nicht mehr als Auftraggeber-Daten im Sinne des Vertrags gelten.

Dieser AV-Vertrag bildet in Verbindung mit den jeweils erforderlichen Anlagen einen Einzel-AV-Vertrag pro Hauptvertrag. Gibt es mehrere Hauptverträge, kann es erforderlich sein, dass die Anlagen 1 bis 4 mehrfach bzw. pro Hauptvertrag ausgefüllt werden müssen.

(2) Fernwartung

Falls eine Fernprüfung/-wartung Teil eines Hauptvertrags ist und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, wird Anlage 5 Bestandteil des jeweiligen Einzel-AV-Vertrages.

(3) Schweigepflicht

Sofern im Rahmen eines Hauptvertrages personenbezogene Daten verarbeitet werden, die der Schweigepflicht gemäß § 203 StGB unterliegen, wird Anlage 5 Bestandteil des jeweiligen Einzel-AV-Vertrages.

## § 2 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen als Verantwortlicher der Verarbeitung im Sinne des Art. 4 Nr. 7 DSGVO allein verantwortlich. Dieses gilt insbesondere für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach den Art. 12 bis 22 DSGVO.

(2) Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (IT-Systemen) im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Der Auftragnehmer ist für die Einhaltung der jeweils für ihn als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO einschlägigen Datenschutzvorschriften, insbesondere des Art. 28 DSGVO, verantwortlich.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

## § 3 Weisungsbefugnis des Auftraggebers

(1) Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Die Weisungen sind vom Auftragnehmer, sowie vom Auftraggeber in schriftlicher Form oder in Textform zu dokumentieren.

(2) In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen bestätigt der Auftraggeber im Nachgang unverzüglich (mind. Textform). Die weisungsberechtigten Personen sind im Bedarfsfall in Anlage 2 aufgeführt.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung, solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## § 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – zu verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der zuständigen Aufsichtsbehörde.

Hierzu gehören

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen. Diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. den Aufsichtsbehörden gegenüber nachweisen;

b) die Verpflichtung, Verstöße des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen oder weiterer vom Auftragnehmer beauftragter Auftragsverarbeiter gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen, unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DSGVO;

c) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung, mit allen ihm zur Verfügung stehenden Informationen;

d) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen der Aufsichtsbehörde.

(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten Befugten zur Vertraulichkeit und falls erforderlich auf das Fernmeldegeheimnis (§ 3 TDDDG) verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Hauptvertrages fort.

(4) Der Auftragnehmer verpflichtet sich, den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu unterstützen, ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen und Anfragen von Betroffenen unverzüglich an den Auftraggeber weiterzuleiten.

(5) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 2 DSGVO. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung. Auf Anfrage des Auftraggebers stellt der Auftragnehmer dem Auftraggeber alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO benötigt werden.

(6) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden. Legt der Auftragnehmer unter Verstoß gegen die DSGVO Zwecke und Mittel selbst fest, gilt er in Bezug auf die Verarbeitung als Verantwortlicher.

(7) Die Erhebung, Verarbeitung oder Nutzung von Daten auf privaten Endgeräten ist nicht gestattet.

(8) Eine Verarbeitung außerhalb der Räumlichkeiten des Auftragnehmers (z.B. im Homeoffice) ist nur mit Zustimmung des Auftraggebers (mind. Textform) zulässig. Für die Beurteilung der Sicherheit der Verarbeitung stellt der Auftragnehmer dem Auftraggeber vorab alle Informationen, insbesondere einen detaillierten Nachweis zur IT-Sicherheit und Richtlinien zur Arbeit im Homeoffice (z.B. Dienstanweisungen oder Betriebsvereinbarungen) zur Verfügung.

(9) Sollten die personenbezogenen 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

(10) Der Auftragnehmer verpflichtet sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

(11) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

## § 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die Festlegung des Schutzniveaus obliegt dem Auftraggeber und wird anhand der Kriterien in Anlage 3 festgelegt.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

## § 6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zur Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Angaben hinsichtlich der Benennung eines Datenschutzbeauftragen (sofern erforderlich) oder eines Ansprechpartners für Fragen zum Datenschutz, siehe im Bedarfsfall Anlage 2.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 8 dieses Vertrages (Dokumentationspflicht, z.B. technische Einrichtung; alle Vertraulichkeitsverpflichtungen von Personen, die Daten verarbeiten; alle Auftragsverarbeitungsverträge von den Unterauftragsdatenverhältnissen).

f) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

## § 7 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern unter den nachfolgenden Bedingungen zu.

(2) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(3) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die unter trust.voize.ai/subprocessors aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Im Falle von Änderungen wird die Seite aktualisiert.

(4) Der Auftragnehmer informiert den Auftraggeber immer mindestens **2 Wochen** vor der Auslagerung über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(5) Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Den Unterauftragnehmern werden in Form eines Vertrages dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.Sofern eine Drittlandübertragung relevant ist bzw. nicht ausgeschlossen werden kann, darf dieses nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(6) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

## § 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichende Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen vor Ort durchzuführen oder im Einzelfall durch zu benennende Prüfer durchführen zu lassen. Die Prüfung durch Dritte darf nicht durch direkte Konkurrenten des Auftragnehmers durchgeführt werden.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers überzeugen kann (Dokumentationspflicht, z.B. technische Einrichtung; alle Vertraulichkeitsverpflichtungen von Personen, die Daten verarbeiten; alle Auftragsverarbeitungsverträge von den Unterauftragsdatenverhältnissen). Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

## § 9 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt und sind streng untersagt. Hierfür bedarf es einer vorherigen schriftlichen (mindestens Textform) Genehmigung des Auftraggebers. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(4) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer

a) sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,

b) erstellte Verarbeitungsergebnisse,

c) Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen

dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Auftraggebers beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen und mindestens 3 Jahre aufzubewahren.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen, jedoch mindestens 3 Jahre über das Vertragsende hinaus, aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(6) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung (mindestens Textform) über die Kostentragung.

(7) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

## § 10 Leistungsort

(1) Die konkreten Angaben zum Leitungsort sind in Anlage 1 festgelegt.

(2) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU/EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

(4) Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. „Drittstaat“ erbringen möchte, die Leistungserbringung dorthin zu verlagern plant oder die Übertragung von Daten aufgrund des Einsatzes von Subunternehmen in Drittstaaten möglich ist, wird der Auftragnehmer zuvor die schriftliche Zustimmung (mindestens Textform) durch den Auftraggeber einholen.

(6) Sofern die Datenübertragung bzw. Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(7) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

## § 11 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

## § 12 Laufzeit und Kündigung

(1) Die Laufzeit des jeweiligen Einzel-AV-Vertrags richtet sich nach der Laufzeit des entsprechenden Hauptvertrages. Der Auftraggeber kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder bewusst und unbegründet nicht ausführen will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Dies gilt insbesondere bei der Nichteinhaltung der Pflichten aus Art. 28 DSGVO.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages, z. B. bei Beendigung des Hauptvertrages, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

## § 13 Haftung

Für die Haftung für den Ersatz von Schäden, den ein Betroffener dadurch erleidet, dass personenbezogene Daten im Rahmen dieser vertraglichen Auftragsverarbeitung unrechtmäßig verarbeitet werden, gilt die Regelung des Art. 82 DSGVO.

## § 14 Sonstiges und Allgemeines

(1) Soweit dieser Vertrag von dem Hauptvertrag abweichende Regelungen trifft, gehen die Regelungen des Auftragsverarbeitungsvertrages diesen vor.
(2) Gerichtsstand ist der Sitz des Auftraggebers.
(3) Es gilt deutsches Recht.
(4) Änderungen und Ergänzungen dieses Vertrages und seiner Anlagen bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Ergänzung oder Änderung handelt.
(5) Sollten sich einzelne Klauseln im Laufe der Zeit als unwirksam erweisen, so berührt dies die Wirksamkeit des übrigen Auftragsverarbeitungsvertrages nicht.

# Anlage(n)

Anlage 1: Gegenstand, Art, Zweck und Schutzniveau der betroffenen Daten

Anlage 2: Weisungsbefugte Personen sowie Datenschutzbeauftragter/Ansprechpartner

Anlage 3: Technische und organisatorische Maßnahmen

Da die Inhalte und die Erforderlichkeit der Anlagen 4 bis 6 von einzelnen Faktoren der Verarbeitung abhängig sind, wird die Zuordnung der Anlagen zum jeweiligen Hauptvertrag in Anlage 1 festgelegt.

# Anlage 1: Gegenstand, Art, Zweck und Schutzniveau der betroffenen Daten

(1) Dieser Auftragsverarbeitungs-Vertrag (Einzel-AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertrag/Angebot/Leistungsvereinbarung (Hauptvertrag) beschriebenen Auftragsverarbeitung ergeben.

(2) Gegenstand der Verarbeitung

| **Dienstleistung (Gegenstand der Verarbeitung)** | **Bereitstellung, Betrieb und Verfügbarhalten der Dokumentationslösung voize für die digitale Pflegedokumentation** |
|---|---|
| Ort der Verarbeitung | ☒ Bundesrepublik Deutschland<br>☒ Europäische Union / Europäischer Wirtschaftsraum<br>☐ Drittland |
| Art und Zweck der Verarbeitung | 1. Software as a Service für die Realisierung (je nach Modulnutzung, Details siehe unten) von:<br>**Modul (a) - Kernfunktion**: Lokale Spracherkennung und Dokumentation, Zuordnung von Dokumentationseinträgen zu Pflegeakten<br>**Modul (b) - Optional**: Gehostete KI-Verarbeitung (textbasiert)<br>**Modul (c) - Optional**: Gehostete KI-Verarbeitung (audiobasiert)<br>**Modul (d) - Optional**: Qualitätsverbesserung (KI-Learning)<br>2. Fernwartung:<br>- Falls vereinbart, Supportleistungen. |

| | |
|---|---|
| Kategorien betroffener Personen | - Mitarbeitende<br>- Bewohner/Klienten/Patienten |

Die Verarbeitungstätigkeiten richten sich nach der Nutzung durch den Verantwortlichen. Es gelten entsprechend der Nutzung die nachfolgend beschriebenen Module.

---

# Modul (a): Kernfunktion — Lokale Spracherkennung und Dokumentation

Die direkte Pflegedokumentation und die damit verbundenen Sprachdaten werden auf dem mobilen Endgerät aufgezeichnet und im Arbeitsspeicher gehalten. Die lokale KI analysiert die Sprachdaten und setzt den erkannten Text in entsprechende Formulare ein. Eine Verarbeitung über voize-Server findet in diesem Anwendungsfall nicht statt.

**Modul (a) ist Bestandteil der Kernfunktion und für alle Auftraggeber aktiv. Einzelne lokale Kernfunktionen des Moduls (a) können durch gehostete Funktion des Moduls (c) ersetzt und/oder durch die Module (b) und (d) ergänzt werden.**

---

# Modul (b): Optional — Gehostete KI-Verarbeitung (textbasiert)

Sofern der Auftraggeber die gehosteten textbasierte KI-Funktionen nutzt, werden pseudonymisierte Dokumentationstexte zur Verarbeitung an den gehosteten (serverseitigen) Inferenzdienst des Auftragnehmers übermittelt. Zu den textbasierten Funktionen zählen insbesondere:

- Qualitätsverbesserung von Dokumentationstexten (Grammatikkorrektur)
- Extraktion und Strukturierung von Dokumentationsinhalten (z.B. Formularbefüllung, SIS-Analyse)
- Klassifikation und Zuordnung von Dokumentationseinträgen
- KI-gestützte Assistenzfunktionen (z.B. Gruppenangebote, inklusive Sprache)

**Pseudonymisierung:** Vor der Übertragung an den gehosteten Dienst werden die Texte lokal auf dem Endgerät pseudonymisiert, d.h. alle erkannten personenbezogenen Daten werden automatisch durch

Pseudonyme ersetzt (z.B. „Frau Müller" → „[RESIDENT_a1b2c3]"). Die Zuordnungstabelle verbleibt ausschließlich im Endgerät und wird nicht an den Server übertragen. Der gehostete Dienst hat zu keinem Zeitpunkt Zugriff auf die Klarnamen der betroffenen Personen. Die Rückführung der Pseudonyme in Klarnamen erfolgt ausschließlich auf dem Endgerät nach Empfang der Antwort.

**Transiente Verarbeitung:** Die übermittelten Daten werden auf dem Server ausschließlich flüchtig im Arbeitsspeicher verarbeitet. Inhalte von Anfragen und Antworten werden zu keinem Zeitpunkt in Anwendungslogs, Zugriffsprotokolle oder Metriken geschrieben.

---

## Modul (c): Optional — Gehostete KI-Verarbeitung (audiobasiert)

Sofern der Auftraggeber anstelle der lokalen Kernfunktion Audiotranskription (Modul a) die gehostete Audiotranskription nutzt, werden die Sprachaufzeichnungen zur Transkription an den gehosteten (serverseitigen) Inferenzdienst des Auftragnehmers übermittelt. Zusätzlich wird eine Liste der im Dokumentationskontext bekannten Personennamen (Bewohner/Klienten/Patienten) übertragen, um die Erkennungsgenauigkeit zu verbessern. Die übermittelte Namensliste umfasst die Namen der Bewohner/Klienten der aktuell ausgewählten Einrichtung bzw. Organisationseinheit, in der die dokumentierende Pflegekraft arbeitet. Dabei werden die im Kundensystem konfigurierten Berechtigungen berücksichtigt, sodass nur Namen übertragen werden, auf die die jeweilige Pflegekraft auch Zugriff hat.

**Keine Pseudonymisierung:** Mit Modul (c) kann die Audiotranskription auf die Serverseite verlagert werden. Die Pseudonymisierung von voize basiert aber gerade auf der Audiotranskription. Insofern erfolgt hier keine lokale Pseudonymisierung auf dem Endgerät.

**Transiente Verarbeitung:** Die Audiodaten werden auf dem Server ausschließlich flüchtig im Arbeitsspeicher verarbeitet. Die Audiodaten selbst werden nach Abschluss der Transkription nicht gespeichert. Inhalte von Anfragen und Antworten werden zu keinem Zeitpunkt in Anwendungslogs, Zugriffsprotokolle oder Metriken geschrieben.

---

## Modul (d): Optional — Qualitätsverbesserung (KI-Learning)

Stimmt der Auftraggeber zu und willigt die dokumentierende Pflegekraft ein, dann werden die Sprachaufnahmen im Endgerät hinsichtlich der Inhalte pseudonymisiert und dem Auftragnehmer für die Qualitätssicherung und -verbesserung insbesondere zum KI-Learning bereitgestellt. Unter dieser Bedingung überprüft der Auftragnehmer die Qualität des Systems laufend und passt dieses gegebenenfalls an.

Sollte zum Zeitpunkt der Aufnahme keine Internetverbindung bestehen, werden die Sprachdateien lokal auf dem Smartphone zur späteren Synchronisation gespeichert. Sobald eine Internetverbindung besteht, erfolgt die Übertragung der pseudonymisierten Daten auf den voize-Server.

**Pseudonymisierung:** Vor der Übertragung an den Dienstleister werden die Audiodateien lokal auf dem Endgerät pseudonymisiert, d.h. alle erkannten personenbezogenen Daten werden im Audiostream durch eine zufällig lange Leerstelle maskiert. Der Auftragnehmer ist nicht in der Lage, diese Pseudonymisierung aufzulösen und die enthaltenen Diagnosen und Befunde einer konkreten Person zuzuordnen. Die Herstellung des Personenbezuges zur einsprechenden Pflegekraft ist nicht gänzlich auszuschließen, so dass hierfür von der Pflegekraft eine Einwilligung vor der Nutzung des Systems eingeholt wird. Die Grundsätze der DS-GVO werden hierbei berücksichtigt. Bei Nichterteilung der Einwilligung erfolgt kein KI-Learning.

---

## Fernwartung

Fernwartung der Systeme per z.B. Teamviewer. Siehe Anlage 4.

---

# Art der Datenkategorien

Die nachfolgende Tabelle beschreibt die Datenkategorien, die im Rahmen der vorstehend beschriebenen Module verarbeitet werden. Nicht alle Datenkategorien werden in jedem Modul verarbeitet.

| Datenkategorie | Erläuterung | Beispiele | Module |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Personenstammdaten** | Grundlegende Personendaten | Name, Geburtsdatum, Anschrift | (a), (c), (d) |
| **Bewohnerdaten** | Daten, die sich auf die Wohn- und Betreuungsstruktur beziehen | Zugehörigkeit zu Wohngruppe und Organisationseinheit | (a) |
| **Gesundheitsdaten** | Medizinische und pflegerische Dokumentation | Vitalwerte, Medikamentengabe | (a), (b)*, (c), (d) |
| **Dokumentationsdaten** | Informationen zur Dokumentation | Strukturierte Informationssammlung (SIS) | (a), (b)* |
| **Personaldaten** | Daten, die sich auf die Anstellung beziehen | Zugehörigkeit zu Organisationseinheit, Zuständigkeits- und Verantwortungsbereich, Berufsbezeichnung | (a) |
| **Kontaktdaten** | Daten, die dazu verwendet werden, eine Person zu erreichen oder mit ihr zu kommunizieren | Name mit Adressdaten, E-Mail-Adresse, Telefonnummer | (a) |
| **Nutzungsdaten** | Daten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von digitalen Diensten zu ermöglichen (§ 2 TDDDG) | Technische Nutzungsdaten wie URL, Zeitpunkt und Dauer des Zugriffs, Geräte-Informationen, IP-Adresse; Workflow- und Prozessdaten | (a), (b), (c) |

| | | | |
|---|---|---|---|
| **Zugangsdaten** | Persönliche Daten, die den Zugang zum System erlauben | Kontoname und Kennwort | (a) |
| **Zugriffsrechte** | Lese-, Schreib- und Löschrechte | | (a) |
| **Audiodaten** | Sprachaufzeichnungen | | (a), (c), (d) |
| **Supportdaten** | Die für eine Supportanfrage verarbeiteten Daten | Kontaktdaten, Beschreibung des Problems, Situationsbeschreibungen, Lösungsvorschläge | Fernwartung |

* In Modul (b) werden Gesundheitsdaten und Dokumentationsdaten in pseudonymisierter Form verarbeitet (Personennamen durch Pseudonyme ersetzt, siehe Modul (b)).

# Leistungsort

Die Liste der aktuellen Unterauftragsverarbeiter inklusive der Leistungsorte findet sich unter https://voize.de/unterauftragnehmer

Der Auftragnehmer wird die vertraglichen Leistungen

- in Deutschland
- in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR)

erbringen.

Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen sowohl in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) als auch unter Umständen in einem Drittland. Siehe dazu die Unterauftragnehmer-Übersicht unter voize.de/unterauftragnehmer.

Erfolgt eine Leistungserbringung durch einen Unterauftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen nach.

Zu dieser Verarbeitung (Einzel-AV-Vertrag) gehörende Anlagen

- Anlage 3: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen
- Anlage 4: Fernwartung
- Anlage 5: Schweigepflicht gemäß § 203 StGB

# Anlage 3: Technische und organisatorische Maßnahmen

# I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

## 1. Zutrittskontrolle (Räume und Gebäude)

*Ziel: Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.*

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Schliessanlage – manuell und per Chip
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel
- Videoüberwachung des Geländes
- Gesicherter Serverraum
- Besucher werden ständig begleitet
- Sorgfältige Auswahl der Reinigungskräfte
- Zugangsregelung zu sensiblen Raumen
- Zoneneinteilung
- Gehostete KI-Verarbeitung (Module (b), (c)): Die serverseitige Verarbeitung erfolgt in Rechenzentren von Amazon Web Services (AWS) in der Region eu-central-1 (Frankfurt, Deutschland). AWS betreibt diese Rechenzentren unter ISO 27001-Zertifizierung mit physischen Sicherheitsmassnahmen einschliesslich biometrischer Zugangskontrollen, Videouberwachung, Einbruchserkennung und 24/7-Sicherheitspersonal. Der Auftragnehmer hat keinen physischen Zugang zu den Rechenzentren.

## 2. Zugangskontrolle (IT-Systeme und Anwendungen)

*Ziel: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

- Login per Benutzername + Passwort
- Einsatz von 2-Faktor-Authentifizierung
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z.B. bei Eintritt, Anderung, Austritt)

- Sorgfältige Personalauswahl - Auswahl von Reinigungspersonal und Sicherheitspersonal nach definierten Unternehmensanforderungen
- Verschlüsselung von Datenträgern
- Einsatz einer Firewall
- Einsatz eines Anti-Virus-Software
- Automatische Desktopsperre mit Kennwort
- Verschlüsselung von Endgeräten
- Protokollierung von An- und Abmeldungen
- Trennung von Produktiv- und Testsysteme
- Richtlinie zum Arbeiten im Homeoffice
- Richtlinie "Clean-Desk"
- Gehostete KI-Verarbeitung (Module (b), (c)): Zugriff auf den gehosteten Konferenzdienst erfolgt ausschließlich über authentifizierte API-Aufrufe. Jede Anfrage wird mit einem JWT-Bearer-Token (OAuth2, Auth0) authentifiziert. Nicht-authentifizierte Anfragen werden abgelehnt.
- Die Verwaltung der Serverinfrastruktur (Kubernetes-Cluster) ist durch rollenbasierte Zugriffskontrolle (RBAC) abgesichert. Administrative Zugriffe erfordern Multi-Faktor-Authentifizierung und werden protokolliert.
- Die interne Kommunikation zwischen Diensten erfolgt über TLS-verschlüsselte Verbindungen mit öffentlicher PKI-Zertifikats Infrastruktur. Der Zugriff auf interne Dienste wird durch eine Zero-Trust-Netzwerkarchitektur (ZTNA) abgesichert.

## 3. Zugriffskontrolle (Auf Daten und Informationen)

*Ziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten, personenbezogenen Daten Zugang haben.*

- Aktenschredder der Stufe 3 (cross cut)
- Protokollierung von Zugriffen auf Anwendungen, konkret bei Eingabe, Änderung und Löschung von Daten
- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts
- Passwortrichtlinien - Festlegung von Lange, Komplexität und Wechselhäufigkeit
- Sichere Aufbewahrung - Gesicherte Aufbewahrung aller Datenträger
- Verschlüsselung von Datenträgern
- Verschlüsselung von Smartphones

- Zugriff auf die erfassten Daten haben ausschließlich autorisierte Mitarbeiter:innen von voize
- Minimale Anzahl von Administratoren
- Admins haben einen zusätzlichen User-Account mit "nur" einfachen Benutzerrechten
- Gehostete KI-Verarbeitung (Module (b), (c)): Mandanten Isolation – Die Organisation des Auftraggebers wird aus dem JWT-Token extrahiert und als Mandanten Kennung verwendet. Anfragen werden ausschließlich mit den für den jeweiligen Mandanten freigegebenen KI-Modellen verarbeitet. Ein mandantenüberschreitender Datenzugriff ist technisch ausgeschlossen.
- Die API-Zugriffe sind durch OAuth2-Berechtigungsbereiche (Scopes) nach dem Prinzip der geringsten Berechtigung (Least Privilege) eingeschränkt.
- Entwickler und Administratoren des Auftragnehmers haben keinen Zugriff auf Anfrageinhalte (Texte, Audiodaten), da diese ausschließlich flüchtig im Arbeitsspeicher der Server-Prozesse verarbeitet werden und nicht in Logs, Datenbanken oder sonstige persistente Speicher geschrieben werden.

## 4. Trennbarkeit

*Ziel: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.*

- Logische Mandantentrennung - Softwareseitige Mandantentrennung
- Festlegung von Datenbankrechten
- Physikalische Trennung der Daten - Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem
- Sandboxing (Testumgebung)
- Im Training eines KI-Modells wird auf Basis eines Datensatzes ein statistisches Modell erstellt. In diesem Modell sind die Daten selbst nicht mehr direkt enthalten, sondern lediglich das Erlernte
- Gehostete KI-Verarbeitung (Module (b), (c)): Die serverseitige KI-Verarbeitung erfolgt in einem dedizierten Kubernetes-Namespace, der von anderen Diensten des Auftragnehmers getrennt ist. Mandanten werden über JWT-basierte Organisationskennungen in den Metriken und Protokollen unterschieden. Die Verarbeitung selbst ist zustandslos – es gibt keine mandantenspezifischen Datenspeicher auf der Serverseite.

## 5. Pseudonymisierung

*Ziel: die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.*

- Trennung Kontaktdaten
- Trennung Stammdaten - Trennung von Kundenstammdaten und Auftragsdaten
- Dokumentationstexte werden bei der Nutzung der App aufgezeichnet. Diese Sprachdateien enthalten Daten, die direkt auf dem Smartphone pseudonymisiert werden. Patientennamen werden aus der Tonspur extrahiert. Nach der Extraktion kann kein Bezug zwischen Person und Befund mehr hergestellt werden. Die Trennung von Anrede, sowie Vor- und Nachnamen verhindert, dass Patienten identifiziert werden können
- Nach der Ubertragung der Daten in die voize-Cloud erfolgt eine manuelle, stichpunktartige Verifizierung der eingesprochenen Daten, um sicherzustellen, dass kein Personenbezug (Patient) mehr vorhanden ist.
- On-Device-Pseudonymisierung bei gehosteter KI-Verarbeitung (Modul (b)): Bei textbasierten KI-Funktionen (z.B. Grammatikkorrektur, Formularbefüllung, SIS-Analyse, Klassifikation) werden sämtliche erkannten Personennamen vor der Übertragung an den gehosteten Dienst auf dem mobilen Endgerät durch nicht-rückverfolgbare Pseudonyme ersetzt (z.B. "Frau Müller" -> "[RESIDENT_a1b2c3]"). Die Zuordnungstabelle verbleibt ausschließlich im Arbeitsspeicher des Endgeräts und wird nicht persistiert oder an den Server übertragen. Der gehostete Dienst hat zu keinem Zeitpunkt Zugriff auf die Klarnamen. Die Rückführung der Pseudonyme in Klarnamen erfolgt ausschließlich auf dem Endgerät nach Empfang der Antwort.
- Keine Pseudonymisierung bei gehosteter Audiotranskription (Modul (c)): Bei der audiobasierten Transkription ist eine Pseudonymisierung vor der Übertragung technisch nicht moglich, da die Pseudonymisierung gerade auf der Transkription basiert. Die Audiodaten und die übermittelte Namensliste konnen daher personenbezogene Daten und Gesundheitsdaten im Sinne des Art. 9 DSGVO enthalten. Zum Schutz dieser Daten gelten die in Abschnitt 5a beschriebenen Massnahmen zur transienten Verarbeitung sowie die Einschrankung des Verarbeitungsorts auf die Bundesrepublik Deutschland (siehe Abschnitt 6).

## 5a. Transiente Verarbeitung bei gehosteter KI-Verarbeitung

*Ziel: Gewährleistung, dass personenbezogene Daten bei der gehosteten KI-Verarbeitung (Module (b), (c)) ausschließlich flüchtig im Arbeitsspeicher verarbeitet und nicht dauerhaft gespeichert werden.*

- **Synchrone Verarbeitung im Arbeitsspeicher** – Inferenzanfragen (Text und Audio) werden synchron im Arbeitsspeicher des Servers verarbeitet. Die gesamte Verarbeitung erfolgt im Rahmen eines einzelnen HTTP-Anfrage-Antwort-Zyklus. Es werden keine Nachrichtenwarteschlangen (Message Queues), Wiederholungspuffer (Retry Buffers) oder Zwischenspeicher fur Anfrageinhalte eingesetzt. Die Verarbeitungsdauer beträgt typischerweise 0,1–30 Sekunden pro Anfrage. Nach Rückgabe der Antwort wird der für die Anfrage reservierte Arbeitsspeicher freigegeben.
- **Kein Logging von Anfrageinhalten** – Inhalte von Anfragen und Antworten (Texteingaben, Modellergebnisse, Audiodaten, Transkriptionsergebnisse, Namenslisten) werden zu keinem Zeitpunkt in Anwendungslogs, Zugriffsprotokolle, verteilte Traces oder Metriken geschrieben. Dies wird sichergestellt durch: (1) keine Konfiguration von Request-Body-Logging im Anwendungs-Framework, (2) zentralisierte Fehlerbehandlung, die Anfrageinhalte aus Fehlermeldungen entfernt, (3) Zugriffsprotokolle des Reverse-Proxy, die ausschliesslich Metadaten (URL-Pfad, HTTP-Methode, Statuscode, Latenz) enthalten.
- **Arbeitsspeicherbegrenzung und Swap-Schutz** – Sämtliche Server-Prozesse werden mit festen Arbeitsspeichergrenzen betrieben, die durch das Container-Orchestrierungssystem (Kubernetes) erzwungen werden. Swap-Speicher ist deaktiviert. Bei Überschreitung der Speichergrenze wird der Prozess beendet (OOMKill) und sämtlicher Arbeitsspeicher freigegeben – eine Auslagerung von Anfragedaten auf die Festplatte findet nicht statt.
- **Keine Speicherabbilder (Crash-Dumps)** – Es ist keine automatische Erzeugung von Speicherabbildern (Core-Dumps, Heap-Dumps, JVM-Heap-Dumps) konfiguriert. Es werden keine Diagnose-Agenten oder Crash-Dump-Sammler eingesetzt. Bei einem Prozessabbruch wird der Arbeitsspeicher einschließlich aller darin befindlichen Anfragedaten vom Betriebssystem freigegeben, ohne auf die Festplatte geschrieben zu werden.
- **Keine temporären Dateien** – Audiodaten und Textinhalte werden zu keinem Zeitpunkt als temporäre Dateien auf die Festplatte geschrieben. Audiodaten werden als Byte-Arrays im Arbeitsspeicher empfangen und direkt an das Transkriptionsmodell übergeben. Textanfragen werden aus dem JSON-Format im Arbeitsspeicher geparst. Der Inferenzdienst verfugt uber keine beschreibbaren Festplatten-Volumes (ausschließlich schreibgeschützte Konfigurationsdaten).
- **Kein serverseitiger Wiederholungsmechanismus** – Der Server wiederholt fehlgeschlagene Anfragen nicht und puffert keine Anfragedaten für spätere Verarbeitung. Bei einem Fehler wird dem Client ein Fehlercode zurückgegeben; die Entscheidung über eine Wiederholung liegt beim Client. Es werden zu keinem Zeitpunkt Anfragedaten über die Dauer der synchronen Verarbeitung hinaus vorgehalten.

### 5b. Clientseitige Schutzmassnahmen bei gehosteter KI-Verarbeitung

*Ziel: Gewährleistung, dass auch auf dem mobilen Endgerät keine unbeabsichtigte Persistierung von Anfrage- oder Antwortdaten im Zusammenhang mit der gehosteten KI-Verarbeitung erfolgt.*

- **Fehlerberichterstattung (Crash-Reporting)** – Der auf dem Endgerät eingesetzte Fehlerberichterstattungsdienst (Sentry) zeichnet ausschliesslich die URL und HTTP-Methode von Netzwerkanfragen auf, nicht jedoch den Inhalt von Anfragen oder Antworten. Es werden keine Session-Replays an den Fehlerberichterstattungsdienst übertragen.

## II. Integritat (Art. 32 Abs. 1 lit. b DSGVO)

### 6. Weitergabekontrolle

*Ziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.*

- E-Mail-Verschlüsselung
- Monitoring der Zugriffe und Abrufe
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von aussen
- TLS-Verschlüsselung mit öffentlicher PKI-Zertifikatsinfrastruktur für die interne Kommunikation zwischen Diensten (z.B. API-Server zu KI-Modell-Backend). Der Zugriff wird durch eine Zero-Trust-Netzwerkarchitektur (ZTNA) abgesichert – jeder Dienst muss sich authentifizieren, unabhängig vom Netzwerkstandort.

### 7. Eingabekontrolle

*Ziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.*

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.
- Alle Daten liegen passwortgeschützt auf dem Server - jeglicher Zugriff wird protokolliert.
- Alle Daten werden ausschließlich zur Verbesserung der künstlichen Intelligenz (KI)- Modelle der Spracherkennung und Textanalyse genutzt. Für alle anderen Zwecke sind die Daten gesperrt.
- Gehostete KI-Verarbeitung (Module (b), (c)) – Protokollierung betrieblicher Metadaten: Für jede Inferenzanfrage werden folgende betriebliche Metadaten protokolliert: Zeitstempel, Verarbeitungsdauer (Latenz), HTTP-Statuscode, Modellbezeichnung und -version, sowie die Mandanten-ID (Organisationskennung). Diese Metadaten-Protokolle werden fur maximal 30 Tage aufbewahrt und anschließend automatisch gelöscht. Die Protokolle enthalten keine personenbezogenen Daten und keine Inhalte von Anfragen oder Antworten.
- Fehlerprotokollierung – Fehlermeldungen enthalten eine zufällig generierte Fehler-ID (UUID) zur Nachverfolgung und Korrelation mit Kundenanfragen. Anfrageinhalte (Texte, Audiodaten, Namenslisten) werden nicht in Fehlermeldungen aufgenommen. Fehlermeldungen enthalten ausschließlich die Fehler-ID, die Fehlerklasse und den Stack-Trace der Anwendung.

# III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

## 8. Verfügbarkeitskontrolle

*Ziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.*

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- und Recoverykonzept
- Monitoring der Systeme

- Server werden durch den Auftragsverarbeiter gesichert, dieser ist ISO27001 zertifiziert. Etwaige Sicherheitsmassnahmen sind unter anderem Feuer- und Rauchmeldeanlagen, Feuerlöscher, Serverraumüberwachung, Klimatisierung der Serverräume, USV, Schutzsteckdosenleisten mit eigenen Stromkreisen, Festplatten- und Serverspiegelung
- Gehostete KI-Verarbeitung (Module (b), (c)): Automatische Skalierung – Der Inferenzdienst wird als zustandsloser Dienst mit automatischer Skalierung betrieben. Bei Lastspitzen werden automatisch zusätzliche Instanzen gestartet.
- Gesundheitsüberprüfung – Jede Instanz wird kontinuierlich durch automatisierte Gesundheitsbefragungen (Liveness- und Readiness-Probes) überwacht. Fehlerhafte Instanzen werden automatisch erkannt und durch neue Instanzen ersetzt.
- Da die gehostete KI-Verarbeitung zustandslos und transient erfolgt (keine Persistierung von Anfragedaten), gibt es keinen Datenverlust bei einem Ausfall einzelner Instanzen. Im Fehlerfall erhält der Client einen Fehlercode und kann die Anfrage erneut senden.

### 9. Wiederherstellbarkeit

*Ziel: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.*

- Datenwiederherstellungen - Regelmassige und dokumentierte Datenwiederherstellungen
- Notfallpläne - IT-Notfallpläne und Wiederanlaufpläne
- Ersatz-Festplatten für Server
- Gehostete KI-Verarbeitung (Module (b), (c)): Die zustandslose Architektur des Inferenzdienstes ermöglicht eine schnelle Wiederherstellung im Störungsfall. Neue Instanzen werden automatisch durch das Container-Orchestrierungssystem gestartet und sind innerhalb weniger Minuten betriebsbereit. Eine Wiederherstellung von Anfragedaten ist nicht erforderlich und nicht moglich, da keine Anfragedaten persistent gespeichert werden.

## IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### 11. Regelmäßige Kontrollen, Dokumentation und ggf. Optimierung

- Audits - Durchführung regelmäßiger interner Audits
- Managementsystem Datenschutz - Managementsystem zum Datenschutz
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Restorekonzept inkl. Notfallkontakte
- Bestellung eines externen Datenschutzbeauftragten
- Regelmäßige Penetrationstests
- Gehostete KI-Verarbeitung (Module (b), (c)): Laufendes Monitoring der Serverinfrastruktur mittels verteilter Ablaufverfolgung (Distributed Tracing) und zentralisierter Metrikerfassung. Automatisierte Alarme bei Anomalien (z.B. erhöhte Fehlerraten, ungewöhnliche Latenz, Ressourcenerschöpfung).
- Regelmäßige Überprüfung der Log-Konfiguration, um sicherzustellen, dass keine Anfrageinhalte in Protokolle gelangen (Prinzip der Datenminimierung).

## 12. Kontrolle der Unterauftragnehmer

- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- DSB - Benennung eines Datenschutzbeauftragten
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO
- Gehostete KI-Verarbeitung (Module (b), (c)): Amazon Web Services (AWS) wird als Unterauftragnehmer für die Bereitstellung der Serverinfrastruktur eingesetzt (siehe Unterauftragnehmer-Ubersicht unter voize.de/unterauftragnehmer). AWS verfügt über ISO 27001-, SOC 2- und C5-Zertifizierungen. Die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen durch AWS wird im Rahmen des bestehenden Auftragsverarbeitungsvertrags mit AWS (AWS Data Processing Addendum) sichergestellt und regelmäßig anhand der veröffentlichten Compliance-Berichte überprüft.

# Anlage 4: Fernwartung

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den zuständigen, benannten Mitarbeiter des Auftraggebers durchgeführt.

(2) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.

(3) Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

(4) Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

(6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Freigabe des Auftraggebers einholen.

(8) Tätigkeiten zur Fehleranalyse, bei denen eine Übermittlung der Daten außerhalb des Zuständigkeitsbereiches des Verantwortlichen erforderlich ist, bedürfen der vorherigen Zustimmung des Auftraggebers. Bei Datenabzug der Daten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Daten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Zustimmung des Auftraggebers vorliegt. Daten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.

(9) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden ausschließlich mit ausdrücklicher und dokumentierter Zustimmung des Auftraggebers und unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

# Anlage 5: Schweigepflicht gemäß § 203 StGB

(1) Die Mitarbeiter des Auftragnehmers kommen bei der Ausübung ihrer Tätigkeit mit Daten von Berufsgeheimnisträgern in Berührung. Die Mitarbeiter dürfen sich nur insoweit Kenntnis von fremden Geheimnissen verschaffen, als dies zur Erfüllung der ihnen zugewiesenen Aufgaben erforderlich ist. Ferner sind die Mitarbeiter verpflichtet, über die ihnen bei Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnisse Stillschweigen zu bewahren und diese keinesfalls unbefugt Dritten zugänglich zu machen.

(2) Der Auftragnehmer verpflichtet sich seine Mitarbeiter i.S.d. § 203 Abs. 4 Satz 1 StGB zur Verschwiegenheit zu verpflichten. Die Mitarbeiter machen sich strafbar, wenn sie unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei Ausübung ihrer Tätigkeit oder bei Gelegenheit bekannt geworden ist. Ein Verstoß gegen § 203 Abs. 4 Satz 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Die Pflicht zur Verschwiegenheit erstreckt sich nicht nur auf fremde Geheimnisse, sondern auf alle Tatsachen, die den Mitarbeitern des Auftragnehmers in Ausübung oder aus Anlass ihrer Tätigkeit anvertraut oder bekannt werden. Die Pflicht zur Verschwiegenheit besteht gegenüber jedermann, so auch gegenüber Familienangehörigen, gegenüber Arbeitskollegen, soweit eine Offenbarung nicht aus dienstlichen Gründen erforderlich ist, sowie auch gegenüber demjenigen, der von der betreffenden Tatsache bereits Kenntnis erlangt hat. Die Pflicht zur Verschwiegenheit besteht auch nach Beendigung der Beauftragung uneingeschränkt und zeitlich unbefristet fort.

(3) Dem Auftragnehmer ist bekannt, dass die einem Berufsgeheimnis unterliegenden Daten dem Zeugnisverweigerungsrecht gemäß § 53a StPO unterfallen. Die Ausübung des Zeugnisverweigerungsrechts obliegt dem Berufsgeheimnisträger. Der Auftragnehmer stimmt sich mit dem Auftraggeber und dieser mit dem Berufsgeheimnisträger ab, sofern der Auftraggeber nicht selbst der Berufsgeheimnisträger ist.

(4) Dem Auftragnehmer ist bekannt, dass, sofern in seinem Gewahrsam befindliche Daten einem Berufsgeheimnis unterliegen, diese dem Beschlagnahmeverbot gemäß § 97 Abs. 3 StPO unterliegen. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

(5) Sofern der Auftragnehmer autorisiert ist, in eigener Verantwortung dritte Personen außerhalb des Unternehmens (= Unterauftragnehmer) in die Durchführung der Tätigkeit des Hauptvertrages einzubeziehen und diese im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen erlangen können, hat der Auftragnehmer dafür Sorge zu tragen, dass auch diese Personen oder Unterauftragnehmer unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit verpflichtet werden. Des Weiteren haben der Auftragnehmer und der Unterauftragnehmer gemäß Art. 28 Abs. 4 DSGVO dafür Sorge zu tragen, dass diese Verpflichtungen auch für etwaige Unterbeauftragungen Gültigkeit haben. Kommt der Auftragnehmer seiner Verantwortung zur Weitergabe der Geheimhaltungsverpflichtungen nicht nach, kann er sich selbst nach § 203 Abs. 4 Satz 2 Nr. 2 StGB strafbar machen, wenn der Unterauftragnehmer ein ihm bei Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis unbefugt offenbart.

(6) Der Auftragnehmer speichert keine geheimnisgeschützten Daten von Berufsgeheimnisträgern innerhalb von IT-Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.