Vertrag über die
Verarbeitung personenbezogener Daten

im Sinne des Art. 28 Abs. 3 der Verordnung (EU) 2016/679 (DSGVO)
– Auftragsverarbeitungsvertrag –

im Auftrag

_____

Auftraggeber: Name/Firma

_____

Auftraggeber: Straße, Hausnummer

_____

Auftraggeber: PLZ, Ort

– Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO –
– nachfolgend „Auftraggeber“ genannt –

durch die

VITAS GmbH
Zollhof 7
90433 Nürnberg

– Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO –
– nachfolgend „Auftragnehmer“ genannt –

– nachfolgend jeweils auch „Partei“ bzw. gemeinsam „Parteien“ genannt –

§ 1 | Gegenstand und Dauer der Auftragsverarbeitung

(1) Gegenstand

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen: Das Hosten, (Fern-) Warten, Pflegen und Betreuen von IT- Systemen im Zuge der Bereitstellung von Nutzungslizenzen für eine Plattform für Telefonassistenten in Form einer im Rechenzentrum betriebenen und für den Auftragnehmer über das Internet zugänglichen Software als Software-as-a-Service, die vom Auftraggeber definierte Daten von Anrufern erfasst und verarbeitet, um die telefonische Erreichbarkeit des Auftraggebers zu sichern und die Anliegen der Anrufer zu bearbeiten.

(2) Dauer

Details zum Gegenstand und der Dauer der Verarbeitung ergeben sich jeweils aus der zwischen den Parteien geschlossenen, diesem Vertrag zugrunde liegenden Nutzungsvereinbarung (nachfolgend Hauptvertrag genannt). Vorliegender Vertrag ist rechtlich unselbständig und teilt das rechtliche Schicksal des Hauptvertrags; eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Es ist den Parteien bewusst, dass ohne Vorliegen eines gültigen Auftragsverarbeitungsvertrags keine (weitere) Auftragsverarbeitung durchgeführt werden darf. Eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen.

§ 2 | Konkretisierung des Auftragsinhalts

(1) Art der Verarbeitung

[1]Im Rahmen des Auftrags werden personenbezogene Daten durch den Auftragnehmer im Sinne des Art. 4 Nr. 2 DSGVO verarbeitet. [2]Im Wesentlichen handelt es sich dabei um 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 und die Vernichtung. Für die Verarbeitung wird dem Auftraggeber eine Rufnummer bereitgestellt, über die der Telefonassistent erreichbar ist und automatisiert Anrufe entgegen nimmt, um die telefonische Erreichbarkeit sicherzustellen. Über die bereitgestellte Verwaltungsplattform wird vom Auftraggeber definiert, welche Daten von den Anrufern erhoben werden sollen. Im Verlauf des Gesprächs obliegt es dem Anrufer eigenständig zu entscheiden, welche Informationen bereitgestellt werden. Der Auftragsverarbeiter hat keinen Einfluss auf die übermittelten Daten, weshalb eine Verarbeitung personenbezogener Informationen unterschiedlicher Art möglich ist. Die Verwaltungsplattform dient dabei auch der organisierten Darstellung der definierten Daten, um die Bearbeitung der Anrufe zu erleichtern. Welche Daten vom Anrufer erfragt werden sollen, bestimmt der Auftraggeber bei Konfiguration des Telefonassistenten selbst. Bei cloudbasierten Angeboten kann ein Zugriff zudem im Rahmen eines Fernzugriffes erfolgen.

(2) Zweck der Verarbeitung

Die Datenverarbeitung erfolgt zu folgendem Zweck: Support, Wartung, Hosting und Bereitstellung der Infrastruktur für die abgeschlossene Vertragslaufzeit zur Nutzung einer als Cloud-Service angebotenen Plattform für telefonische Sprachassistenten in Form einer im Rechenzentrum betriebenen und für den Auftraggeber über das Internet zugänglichen Software als Software-as-a-Service, die die telefonische Erreichbarkeit der Auftraggeber sicherstellen soll und die Anliegen der Anrufer strukturiert nach vom Verantwortlichen vorkonfigurierten Nutzerszenarien erfragt und zur weiteren Verarbeitung erfasst.

(3) Ort der Verarbeitung

[1]Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. [2]Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen. [3]Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß § 5 (3) für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(4) Art der Daten

In welchem Umfang und welche Daten vom Anrufer erfragt werden, sowie ob eine Anbindung des Telefonassistenten an weitere Softwares erfolgen soll, bestimmt der Auftraggeber bei Konfiguration des Telefonassistenten vollumfänglich selbst. Ebenfalls bestimmt der Anrufer im Gesprächsverlauf selbst, welche Daten er mitteilen möchte. Daraus ergibt sich, dass personenbezogene Daten verschiedenster Art verarbeitet werden können. Die Datenverarbeitung erfolgt ausschließlich im Auftrag und nach Weisung des Auftraggebers.

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Personenbezogene Daten von Nutzern der Anwendung:

- ☑ Personenstammdaten (z.B. Name, Vorname)*
- ☑ Kontakt-/Kommunikationsdaten (z. B. E-Mail)*
- ☑ IP-Adresse*

Personenbezogene Daten von Anrufern:

- ☐ Vollständiger Name des Anrufers (Vorname, Nachname)
- ☐ Telefonnummer des Anrufers
- ☑ Übermittelte Telefonnummer des Anrufers*
- ☐ Geburtstag des Anrufers
- ☑ Sprachaufzeichnung des Anrufers - biometrische Daten (Art. 4 Nr. 14 DSGVO)*
- ☐ Anliegen des Anrufers
- ☐ Grund für den Terminwunsch
- ☐ ggf. freiwillig mitgeteilte Gesundheitsdaten (Art. 4 Nr. 15 DSGVO)
- ☐ Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ ggf. freiwillig mitgeteilte Daten, die unter das Berufsgeheimnis nach § 203 Abs. 1 und 2 StGb fallen

**Diese Datenkategorien müssen zur Bereitstellung der Dienstleistung immer verarbeitet werden.*

Bei der Anbindung des Telefonassistenten an die folgende(n) Software Integration(en)

_____

werden folgende weitere personenbezogene Daten verarbeitet:

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

(5) Kategorien betroffener Personen

Der Kreis der betroffenen Personen ergibt sich aus dem jeweiligen Anwendungsbereich des Telefonassistenten. Es können daher unterschiedliche Personengruppen betroffen sein.

Die Kategorien der durch die Verarbeitung betroffenen Personen können umfassen:

- ☐ Auftraggeber als Kunde der VITAS GmbH
- ☐ Nutzer der VITAS Plattform
- ☐ Kunden des Auftraggebers
- ☐ Interessenten des Auftraggebers
- ☐ Beschäftigte des Auftraggebers (z.B. als Nutzer oder als Anrufer der Plattform)
- ☐ Ansprechpartner des Auftraggebers
- ☐ Anrufer beim Auftraggeber (z.B. interne Fachabteilungen oder externe Kunden)

In Praxen oder Gesundheitseinrichtungen:

- ☐ Patienten des Auftraggebers
- ☐ Neue Patienten (Interessenten)

In Anwalts- oder Steuerberatungskanzleien:

- ☐ Klienten des Auftraggebers
- ☐ Neue Klienten (Interessenten)

§ 3 | Technische und organisatorische Maßnahmen

(1) [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. [2]Bei Akzeptanz durch den Auftraggeber werden die dokumentierten

Maßnahmen Grundlage des Auftrags. [3]Soweit die Prüfung bzw. ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) [1]Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c und lit. e Hs. 1, Art. 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, 2 DSGVO, herzustellen. [2]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 und Dienste. [3]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 [Einzelheiten in Anlage 1].

(3) [1]Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. [2]Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. [3]Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. [4]Wesentliche Änderungen sind zu dokumentieren.

§ 4 | Qualitätssicherung und sonstige Pflichten des Auftragnehmers gem. Art. 28 Abs. 3 S. 1 DSGVO

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags eigene gesetzliche Pflichten eines Auftragsverarbeiters; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) [1]Soweit gesetzlich verpflichtet, benennt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz, die ihre Tätigkeit gemäß Art. 39, 38 DSGVO ausübt. [2]Die Kontaktdaten des benannten Datenschutzbeauftragten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitgeteilt. [3]Sofern der Auftragnehmer nicht zur Benennung eines Datenschutzbeauftragten verpflichtet ist, benennt er einen Ansprechpartner für Datenschutzangelegenheiten, dessen Kontaktdaten dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitgeteilt werden. [4]Sämtliche Änderungen in der Person des Datenschutzbeauftragten bzw. des Ansprechpartners sind dem Auftraggeber unverzüglich anzuzeigen. [5]Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, benennt er gem. Art. 27 DSGVO einen Vertreter in der Union. [6]Die Kontaktdaten des Vertreters sowie sämtliche Änderungen in der Person des Vertreters sind dem Auftraggeber unverzüglich anzuzeigen

b) Der Auftragnehmer gewährleistet gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

c) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung (Art. 29, 32 Abs. 4 DSGVO) des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, Art. 32 DSGVO [Einzelheiten in Anlage 1].

e) Der Auftraggeber und der Auftragnehmer (und ggf. deren Vertreter) arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen (Art. 31 DSGVO).

f) [1]Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über aufsichtsbehördliche Kontrollhandlungen und Maßnahmen zu informieren, soweit sie sich auf diesen Auftrag beziehen. [2]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.

g) 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.

h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

i) Der Auftragnehmer gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 6 dieses Vertrags.

§ 5 | Unterauftragsverhältnisse gem. Art. 28 Abs. 3 S. 2 lit. d DSGVO i.V.m. Art. 28 Abs. 2 und 4 DSGVO

(1) [1]Als Unterauftragsverhältnisse sind Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. [2]Nicht als Unterauftragsverhältnisse sind dagegen solche Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. [3]Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen oder Bewachungsdienste. [4]Gleichwohl ist der Auftragnehmer verpflichtet, auch bei von Dritten erbrachten Nebenleistungen Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. [5]Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

(2) In Übereinstimmung mit der Regelung des Art. 28 Abs. 2 S. 1 DSGVO nimmt der Auftragnehmer keinen weiteren Auftragsverarbeiter (Unterauftragnehmer, Sub-Unterauftragnehmer) ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch, wobei die Bestimmungen zu Unterauftragsverhältnissen sowohl für den Unterauftragnehmer als auch für sämtliche in der Folge in Anspruch genommenen weiteren (Sub-)Unterauftragnehmer (entsprechende) Anwendung finden.

(3) Der Auftraggeber stimmt hiermit der Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste in Anlage I aufgeführt sind, zu. Die Parteien halten Anlage 1 jeweils auf dem neuesten Stand.

(4) [1]Der Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter (Unterauftragnehmer) durch den Auftragnehmer. [2]Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. [3]Dem Auftraggeber steht im Einzelfall ein Recht zu, schriftlich oder in Textform Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. [4]Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. [5]Soweit der Auftraggeber nicht innerhalb von vier Wochen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. [6]Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer diesen Vertrag wie auch gegebenenfalls den Hauptvertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(5) [1]Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. [2]Insbesondere obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag nach Maßgabe des Art. 28 Abs. 4 S. 1 DSGVO auf den weiteren Auftragsverarbeiter zu übertragen.

(6) [1]Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. [2]Gleiches gilt, wenn Dienstleister im Sinne des Abs. 1 Satz 2 eingesetzt werden sollen. [3]Der Auftragnehmer hat für sämtliche Unterauftragnehmer in Drittländern ein Transfer Impact Assessment mit dem Ergebnis durchgeführt, dass ein dem europäischen Datenschutzniveau der Sache nach gleichwertiges Niveau im Sinne der DSGVO gewährleistet ist. [4]Weiterhin hat der Auftragnehmer im Vertrag mit den Unterauftragnehmern in Drittländern die EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 einbezogen.

(7) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der vorherigen ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform) und der vorherigen ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 6 | Kontrollrechte des Auftraggebers gem. Art. 28 Abs. 3 S. 2 lit. h DSGVO

(1) [1]Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer, die nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer stehen dürfen, durchführen zu lassen. [2]Er hat das Recht, sich durch (Stichproben-) Kontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung der Bestimmungen dieses Vertrags durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) [1]Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. [2]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

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder

d) eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit (z. B. nach dem BSI-Grundschutz).

§ 7 | Unterstützungs- und Mitteilungspflichten des Auftragnehmers gem. Art. 28 Abs. 3 S. 2 lit. e und f DSGVO

(1) [1]Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich. [2]Vor diesem Hintergrund ist der Auftragnehmer gleichwohl verpflichtet, den Auftraggeber abhängig von der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner, des Auftraggebers, Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person, das heißt bei der Beantwortung von Anfragen betroffener Personen in Bezug auf die Informationspflichten des Auftraggebers gegenüber den betroffenen Personen, deren Auskunftsrecht, ihrem Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie damit im Zusammenhang stehenden Mitteilungspflichten des Auftraggebers, dem Widerspruchsrecht oder auf automatisierte Entscheidungen einschließlich Profiling zu unterstützen, wenn die betroffene Person entsprechende Rechte geltend macht. [3]Soweit sich die betroffene Person zwecks Geltendmachung eines Rechts unmittelbar an den Auftragnehmer wendet, leitet dieser die Anfragen der betroffenen Person unverzüglich an den Auftraggeber weiter.

(2) [1]Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Auftragsverarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen außerdem bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten, also bei der Erfüllung seiner, des Auftraggebers, gesetzlichen Verpflichtungen zur Datensicherheit, zur Meldung von Datenpannen an die Aufsichtsbehörden und die betroffenen Personen, zur Durchführung von Datenschutz-Folgenabschätzungen sowie zur vorherigen Konsultation der zuständigen Aufsichtsbehörde, sofern dies im Rahmen der Datenschutz-Folgenabschätzung erforderlich ist. [2]Der Auftragnehmer und der Auftraggeber arbeiten auf Anfragen der zuständigen Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben zusammen.

§ 8 | Weisungsbefugnis des Auftraggebers

(1) [1]Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer anderweitigen Verarbeitung verpflichtet ist (Art. 28 Abs. 3 S. 3 lit. a, Art. 29 DSGVO). [2]Im Falle einer solchen Verpflichtung 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) [1]Der Auftragnehmer gewährleistet, dass die Auftragsverarbeitung im Einklang mit den Weisungen des Auftraggebers erfolgt. [2]Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darüber zu informieren; nach einer entsprechenden Mitteilung an den Auftraggeber ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. [3]Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung beim Auftraggeber liegt.

(3) [1]Die Weisungen des Auftraggebers erfolgen grundsätzlich in Schrift- oder Textform. [2]Bei Bedarf kann der Auftraggeber Weisungen auch (fern-)mündlich erteilen. [3](Fern-)Mündlich erteilte Weisungen bestätigt der Auftraggeber unverzüglich in Schrift- oder Textform. Die vollständige Dokumentation der Weisungen hat sowohl durch den Auftraggeber als auch den Auftragnehmer zu erfolgen.

§ 9 | Löschung und Rückgabe von personenbezogenen Daten gem. Art. 28 Abs. 3 S. 2 lit. g DSGVO

(1) [1]Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. [2]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.

(2) [1]Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. [2]Gleiches gilt für Test- und Ausschussmaterial. [3]Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) [1]Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. [2]Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 10 | Verpflichtung zur Geheimhaltung von Berufsgeheimnissen(§ 203 StGB)

(1) Im Rahmen dieses Auftrages können auch Daten verarbeitet werden, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.

(2) Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(3) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

(4) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrechts von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(5) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

(6) Der Auftragnehmer ist berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Des weiteren werden Subunternehmer über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß §97 StPO informiert; dies beinhaltet auch den Hinweis auf das Recht des Berufsgeheimnisträgers über dieses Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

§ 11 | Sonstige Bestimmungen

(1) [1]Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Berufsgeheimnissen, Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. [2]Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

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

(3) [1]Für Nebenabreden ist die Schriftform erforderlich. [2]Dies gilt in gleicher Weise für den Verzicht auf dieses Formerfordernis.

(4) Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Dieser Vertrag gilt auch, wenn und soweit Behörden oder Gerichte abweichend eine gemeinsame Verantwortlichkeit der Vertragsparteien nach Art. 26 DSGVO annehmen.

(6) [1]Sollten sich einzelne Bestimmungen des Vertrags ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, so bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrags im Ganzen hiervon unberührt. [2]An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt. [3]Sollte sich der Vertrag als lückenhaft erweisen, so gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrags entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(7) Der Vertrag unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland unter Ausschluss seiner internationalen Verweisungsnormen.

(8) Ausschließlicher Gerichtsstand bei allen Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragnehmers.

	Nürnberg 24.08.2023
Ort, Datum	Ort, Datum

	DocuSigned by: Thomas Abend 016C5B8A7DB9426...
Auftraggeber	Auftragnehmer

Anlage I - Liste der Unterauftragsverarbeiter

Anlage II - Technische und organisatorische Maßnahmen

ANLAGE I – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Speicherplatz Datenbank / Server:

Name/Firma	Kontakt	Zur Verfügung gestellter Service
Sys Eleven GmbH Boxhagener Str. 80, 10245 Berlin Deutschland	**Madina Utova** datenschutz@syseleven.de Datenschutzbeauftragte	Bereitstellung von Servern und Cloud-Infrastruktur mit Serverstandort in Berlin und Frankfurt
checkdomain GmbH Große Burgstraße 27/29, 23552 Lübeck Deutschland	**Alfahosting GmbH** datenschutz@checkdomain.de Datenschutzbeauftragte	Webhosting, SaaS-Leistungen, Registrar, Domain Name System

Telefon- / Telekommunikationsinfrastruktur:

Zur Bereitstellung von Telefoninfrastruktur und Telefonnummern für den VITAS Telefonassistenten arbeitet VITAS mit zwei Anbietern zusammen. Seit August 2023 wird dabei bei sämtlichen Neukunden sowie in Abstimmung mit Kunden, die hohe Anforderungen an den Datenschutz haben, ausschließlich der Anbieter Open Numbers GmbH eingesetzt.

Name/Firma	Kontakt	Zur Verfügung gestellter Service
Open Numbers GmbH Am neuen Berg 3, 63755 Alzenau Deutschland	**Lorenz Barth** lorenz.barth@opennumbers.de Geschäftsleitung	Bereitstellung der deutschen Telefonnummern und Telefoninfrastruktur mit Serverstandort in Deutschland
Zingaya, Inc. The Lipstick Building 885 Third Avenue, 24th floor. Suite 2402 New York, NY 10022 USA	support@voximplant.com	Bereitstellung von (ausländischen) Telefonnummern und Telefoninfrastruktur mit Serverstandort in Deutschland

Optionale Funktionalitäten:

Eine Übermittlung von Daten an die nachfolgend aufgeführten Unterauftragnehmer erfolgt ausschließlich dann, wenn spezifische Funktionen innerhalb der VITAS Plattform aktiviert und genutzt werden. Diese Funktionen sind in der VITAS Plattform deutlich gekennzeichnet und können erst nach Zustimmung verwendet werden.

Der Auftraggeber behält in der VITAS Plattform die volle Entscheidungsfreiheit, zu bestimmen, ob er von diesen Funktionen Gebrauch machen möchte und ob er damit den Einsatz der nachfolgenden Unterauftragnehmer in der VITAS Plattform genehmigen möchte.

Name/Firma	Kontakt	Zur Verfügung gestellter Service
MessageBird B.V. Trompenburgstraat 2C1079,TX Amsterdam Niederlande	privacy@messagebird.com	Schnittstelle für den SMS-Versand zur Benachrichtigung der Anrufenden aus der VITAS Plattform.
rapidmail GmbH Wentzingerstraße 21, 79106 Freiburg im Breisgau Deutschland	n.moellers@keyed.de Externer Datenschutzbeauftragter	Versand von Transaktionsmails aus der VITAS Plattform zur Benachrichtigung. **Die Übertragung von personenbezogenen Daten lässt sich in der VITAS Plattform aktivieren bzw. deaktivieren.**
OpenAI, L.L.C. 3180 18th St, San Francisco, CA 94110 USA	privacy@openai.com	Schnellerer Abgleich und Zuordnung von Aussagen eines Anrufenden mit vorgegebenen Optionen oder mit FAQ-Informationen des Auftraggebers. **Die Übertragung der Antworten der Anrufer erfolgt ausschließlich in Textform.**
Google LLC (formerly known as Google Inc.) 1600 Amphitheatre Parkway, Mountain View, California 94043 USA	data-access-requests@ google.com Datenschutzbeauftragte	Nutzung der Adresserkennung, ausschließlich Abgleich der durch den Anrufer angegebenen Adresse (Übermittlung als Text). **Keine Übermittlung von weiteren personenbezogenen Daten.**
DeepL SE Maarweg 165, 50825 Köln Deutschland	datenschutz@dhpg.de	Nutzung der Schnittstelle für Übersetzungsdienste zur Bereitstellung eines multilingualen Telefonassistenten.

ANLAGE II – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

In diesem Dokument werden die verbindlichen technischen und organisatorischen Maßnahmen beschrieben, die im Zusammenhang mit den durchgeführten Auftragsverarbeitungsvorgängen zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt wurden. Diese dargestellten Maßnahmen spiegeln das Datenschutz- und Datensicherheitskonzept der VITAS GmbH wider.

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 EU-DSGVO. Die EU-DSGVO verpflichtet Unternehmen, die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt die VITAS GmbH durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen.

Besondere Beachtung in jedem Datenverarbeitungsvorgang finden die Schutzwerte Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit. Für diese Schutzwerte gelten die folgenden informationssicherheitsrelevanten Definitionen:

Vertraulichkeit: Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.

Integrität: Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.

Verfügbarkeit: Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.

Belastbarkeit: Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sein müssen.

Unter Berücksichtigung des

- Stand der Technik
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

werden die folgenden technischen und organisatorischen Maßnahmen umgesetzt, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Auswahl der Maßnahmen werden insbesondere die Risiken berücksichtigt, die mit den Verarbeitungsvorgängen einhergehen.

Zutrittskontrolle:
Der Zugang zu Datenverarbeitungsanlagen, die für die Verarbeitung oder Nutzung personenbezogener Daten eingesetzt werden, ist unbefugten Personen zu verwehren.

Zutrittskontrollsystem - Abschließbare Räume:
Innerhalb des Unternehmens sind alle Räumlichkeiten, in denen ein Zugriff auf personenbezogene Daten möglich ist, mit abschließbaren Vorrichtungen ausgestattet. Die Maßnahmen der Zutrittskontrolle stellen sicher, dass nur befugtes Personal Zugang zu diesen Räumen und Vorrichtungen hat und somit die Vertraulichkeit der personenbezogenen Daten gewährleistet ist.

- Zentral verwaltetes Zutrittskontrollsystem, welches Zutritte protokolliert
- Schließvorrichtungen an Räumlichkeiten
- Tresor

Server - Externer Einsatz:
Im Unternehmen werden externe Server (z.B. in einem Rechenzentrum) angemietet. Die gewählten Rechenzentren verfügen über eine ISO 27001-Zertifizierung und die Lieferanten werden gemäß dem Kriterienkatalogs Cloud Computing C5 gewählt.

Server - Interner Einsatz:
In den Unternehmensräumlichkeiten werden keine Server eingesetzt.

Sicherung des Unternehmensgeländes - Abgrenzung:
Die Unternehmensräumlichkeiten werden vom öffentlichen Bereich abgegrenzt durch:

- Abschließbare Haustüre - Haustürschlüssel
- Bürokomplex - elektronisches Zutrittskontrollsystem
- Büroräume, in denen personenbezogene Daten verwahrt werden - elektronisches Zutrittskontrollsystem oder Schlüssel

Im Auftrag verarbeitete, personenbezogene Daten werden nur digital verarbeitet und nicht in Papierform in den Büroräumlichkeiten verwahrt.

Technisches Mittel: Das Zutrittskontrollsystem basiert auf folgenden technischen Mitteln: - RFID-Chips

Zutrittskontrollsystem - Verwaltung:
Das Zutrittskontrollsystem wird folgendermaßen verwaltet: - Elektronisch

Zugangskontrolle:
Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet oder genutzt werden, ist ausschließlich autorisiertem Personal gestattet. Unbefugten wird der Zugang zu diesen Anlagen untersagt, um die Sicherheit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten.

Tragbare Endgeräte - Zugangssperren: Im Unternehmen verfügen tragbare Endgeräte über Zugangssperren:

- Touch ID
- Passwort
- PIN (Komplexität wird erzwungen)
- Automatische Sperrung der Geräte nach gewissem Zeitablauf ohne Useraktivität

Tragbare Endgeräte - Verschlüsselung: Im Unternehmen werden die Festplatten der tragbaren Endgeräte über eine Festplattenverschlüsselung verschlüsselt (XTS-AES-128-Verschlüsselung).

Passwort-Manager: Im Unternehmen wird verpflichtend für die Mitarbeiter ein Passwort-Manager eingesetzt, der den Einsatz von komplexen Passwörtern vorgibt und bei der sicheren Passwortverwaltung unterstützt.

Über den Passwort-Manager werden komplexe Passwörter vorgeschlagen, die eine Länge von 20 Zeichen haben, mindestens eine Ziffer und mindestens einen Groß- und Kleinbuchstaben enthalten.

Passwort-Manager - Zugangskontrolle: Der eingesetzte Passwort-Manager bietet eine ausreichende Zugangskontrolle mit 2-Faktor-Authentifizierung und eine verschlüsselte Speicherung.

Mitarbeiter - Aufbewahrung sensibler Informationen: Im Unternehmen sind die Beschäftigten verpflichtet worden, personenbezogene Daten beim Verlassen des Arbeitsplatzes verschlossen zu lagern (sog. Clean-Desk-Policy).

Tragbare Endgeräte - Passwortkomplexität: Im Unternehmen werden ausreichend komplexe Passwörter und PINs für die Nutzung von tragbaren Endgeräten gefordert. Die Passwortrichtlinie fordert ein Passwort mit mind. 12 Zeichen, mind. einem Groß- und Kleinbuchstaben, das Kennwort darf in keinem Wörterbuch enthalten sein und es dürfen keine persönlichen Daten enthalten sein.

Authentifizierung - Zwei-Faktor-Authentifizierung: Im Unternehmen wird bei allen Anwendungen, die es ermöglichen, die Zwei-Faktor-Authentifizierung eingesetzt.

Authentifizierung - Single Sign-On Verfahren: Im Unternehmen wird ein Single Sign-On Verfahren eingesetzt.

Zugang zu personenbezogenen Daten in Bereichen mit Publikumsverkehr: Im Unternehmen wird durch Schließvorrichtungen dafür gesorgt, dass personenbezogene Daten in Bereichen mit Publikumsverkehr nicht frei zugänglich sind.

Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Ausgeschiedene Personen - Entzug von Berechtigungen: Im Unternehmen wird sichergestellt, dass sämtliche Zugangsberechtigungen und Zugriffsberechtigungen einer ausscheidenden Person schnellstmöglich gesperrt und ggf. gelöscht werden.

Rollen- und Berechtigungskonzept: Das Unternehmen hat ein Rollen- und Berechtigungskonzept gemäß der ISO 27001-Norm implementiert:

- Zugriffsgruppen und geplanter Zugriff
- Genehmigungsroutinen
- Verwaltung und Dokumentation von differenzierten Berechtigungen sowie regelmäßige Kontrolle

Datenträgerkontrolle

Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Tragbare Datenträger - Verschließbare Behältnisse: Im Unternehmen stehen an allen Arbeitsplätzen verschließbare Behältnisse zur Verfügung, um Unterlagen und Datenträger sicher aufbewahren zu können.

Tragbare Datenträger - MDM: Im Unternehmen wird ein Mobile Device Management für tragbare Endgeräte genutzt. Das MDM ermöglicht eine Fernlöschung von Daten.

Tragbare Endgeräte - Geeignete Aufbewahrung: Im Unternehmen werden Benutzer von tragbaren Endgeräten auf die Einhaltung einer geeigneten Aufbewahrung verpflichtet.

Tragbare Endgeräte - Diebstahlsicherung: Im Unternehmen werden tragbare Endgeräte außerhalb der Nutzungszeiten gegen Diebstahl gesichert.

Datenträgermanagement - Bestandsverzeichnis: Im Unternehmen wird für folgende elektronischen Datenträger ein Bestandsverzeichnis geführt:

- Tablet Computer
- Mobiltelefone
- Laptops

Übertragungskontrolle

Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

Telekommunikation - Verbindung zum Telekommunikationsprovider: Zur Verbindung mit dem Telekommunikationsprovider wird folgende Methode verwendet:

- Reguläre DSL-Verbindung
- Firmeninternes WLAN-Netzwerk
- Separates WLAN-Netzwerk für Gäste
- Zero Trust Network

Verschlüsselung - Alle Übertragungen von Daten ab dem von VITAS betriebenen Telefonendpunkt werden ausschließlich verschlüsselt versendet. Auf die Telefonverbindung vom Anrufer zum Endpunkt hat VITAS keinen Einfluss.

Transportkontrolle
Es ist zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Kommunikation - Digitale Signaturen: Im Unternehmen werden zum Versand von E-Mails digitale Signaturen eingesetzt.

Datenübertragung - Datenträger: Im Unternehmen werden keine Datenträger mit personenbezogenen Daten übermittelt.

Benutzerkontrolle
Es ist zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.

Ausgeschiedene Personen - Rückforderung unternehmenseigener Gegenstände: Im Unternehmen wird sichergestellt, dass sämtliche unternehmenseigenen Gegenstände mit Bezug zu personenbezogenen Daten von einer ausscheidenden Person zurückgefordert werden.

Endgeräte - Richtlinien: Im Unternehmen existiert eine Richtlinie zum Umgang mit Endgeräten gemäß der ISO/IEC 27001.

Telekommunikation - Datenschutz für Telearbeiter: Telearbeiter wurden auf die Einhaltung einschlägiger Datenschutzvorschriften verpflichtet.

Administratoren: Im Unternehmen wurden für alle IT-Systeme und IT-Netze Administratoren sowie deren Stellvertreter bestimmt.

Administratoren - Qualifikation: Im Unternehmen wird sichergestellt, dass IT-Administratoren über ausreichende Qualifikation zur Ausübung ihrer Tätigkeit verfügen.

Administratoren - Spezielle Konten: Im Unternehmen werden spezielle Administratorenkonten eingesetzt.

Mitarbeiter - Maßnahmen:
Um im Unternehmen die Beschäftigten auf die Wichtigkeit des Datenschutzes hinzuweisen und diese gemäß den Erfordernissen zu verpflichten, werden folgende Maßnahmen getroffen:

Verpflichtung der Beschäftigten auf das Datengeheimnis:
- Unternehmensinterne Datenschutz-Richtlinien
- Verpflichtung der Mitarbeiter zur Einhaltung der datenschutzrechtlichen Anforderungen
- Verpflichtung der Beschäftigten auf Vertraulichkeit nach § 203 StGB.

Verpflichtung der Beschäftigten zu Verhaltensregeln:

- Verpflichtung der Mitarbeiter auf die Einhaltung der Grundsätze der Informationssicherheit und Akzeptanz der ISMS-Dokumente

Regelmäßige Schulungen und Sensibilisierungsmaßnahmen

- Jährliche Datenschutzschulung mit Zertifikatsnachweis für jeden Mitarbeiter obligatorisch
- Jährliche Informationssicherheitsschulung mit Zertifikatsnachweis für jeden Mitarbeiter obligatorisch

Administratoren - Ebenen: Im Unternehmen werden die Administratorenkonten auf folgender Ebene eingesetzt:

- Datenbank
- Server
- Mobile Device Management
- VITAS Produkt

Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Externe Dienstleister: Das Unternehmen arbeitet mit externen Dienstleistern zusammen. Es erfolgt eine regelmäßige Lieferantenkontrolle gemäß der ISO/IEC 27001.

- Bestimmung von Lieferantenkategorien
- Sicherheitsrichtlinien für Lieferantenbeziehungen
- Sicherheitsklauseln für Lieferanten

Externe Dienstleister - Weisungen zur Verarbeitung: Im Unternehmen werden Weisungen zur Verarbeitung personenbezogener Daten ausschließlich schriftlich an Auftragsverarbeiter erteilt.

Externe Dienstleister - Auftragsverarbeitungsvertrag: Im Unternehmen wurde mit allen Dienstleistern ein Auftragsverarbeitungsvertrag geschlossen.

Externe Dienstleister - Fernwartung: Im Unternehmen werden keine Fernwartungen durchgeführt.

Speicherkontrolle

Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter, personenbezogener Daten ist zu verhindern.

Mitarbeiter - Fachgerechte Entsorgung personenbezogener Daten: Im Unternehmen sind die Beschäftigten angehalten, personenbezogene Daten fachgerecht zu entsorgen.

Passwortschutz - Passwortliste: Es wird keine unverschlüsselte Passwortliste geführt. Es wird verpflichtend für alle Mitarbeiter ein digitaler Passwortmanager eingesetzt.

Authentifizierung - Datensperrung und -löschung: Im Unternehmen besteht die Möglichkeit auf Antrag personenbezogene Daten zu sperren und zu löschen.

Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten jederzeit verfügbar und besonders gegen zufällige Zerstörung oder Verlust geschützt sind.

Archivierungskonzept - Gesetzliche Aufbewahrungspflicht: Es liegt eine gesetzliche Aufbewahrungspflicht für die archivierten Dokumente vor.

- Security Incident Management System
- Schutz vor Schadsoftware
- Firewall

Zuverlässigkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust abgesichert sind.

IT-Sicherheit - Redundanz kritischer Systeme: Im Unternehmen sind kritische Systeme und ggf. die Infrastruktur redundant ausgelegt.

- Sicherheitskonzept für Software und IT-Anwendungen

Penetrationstest - Regelmäßigkeit: Im Unternehmen werden regelmäßig Belastungstests auf den IT Systemen durch Simulation hoher Belastungen durchgeführt. Regelmäßige Penetrationstests werden geplant und mit unabhängigen Partnern und ggf. in Zusammenarbeit mit Kunden durchgeführt.

Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Sicherungen: Im Unternehmen werden die Sicherungen durchgeführt von:

- Cloud-Anbieter
- Unternehmen
- Dienstleister

Betriebssystem

Es ist zu verhindern, dass Unbefugte Zugriff auf Betriebssysteme erhalten können.

Passwortschutz - Benutzerkonten: Auf Betriebssystemebene wird jedes Benutzerkonto des Betriebssystems durch ein Passwort geschützt.

Administration - Berechtigungskonzept in Test- und Entwicklungsumgebung: Auf Betriebssystemebene wurde ein Berechtigungskonzept in den Test- und Entwicklungsumgebungen umgesetzt.

Anwendungen

Es ist zu verhindern, dass Unbefugte Zugriff auf jegliche Anwendungen erhalten können.

Software - Trennung zwischen Umgebungen: Im Unternehmen gibt es eine Trennung zwischen Produktiv-, Test-, und Entwicklungsumgebungen inkl. der Datenbanken.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
Das Unternehmen hat ein Informationssicherheitsmanagementsystem gemäß der ISO/IEC 27001 implementiert und unterzieht sich einer unabhängigen Prüfung durch eine akkreditierte Zertifizierungsstelle.

- Verfahren für regelmäßige Kontrollen
- Regelmäßige Testtermine
- Notfalltests