GRUNDIG
Business Systems

Vertrag zur Auftragsverarbeitung zwischen

Grundig Business Systems GmbH & Co. KG Emmericher Strasse 17
90411 Nürnberg, Deutschland
– nachfolgend GBS bzw. Auftragnehmer genannt –

und

– nachfolgend Auftraggeber genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) GBS führt die im Anhang 1 beschriebenen Dienstleistungen oder Teile davon für den Auftraggeber durch. Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Gegenstand des Vertrages sind die im Anhang 1 aufgeführten Leistungen, abhängig von den vom Auftraggeber genutzten Produkten des Auftragnehmers. Im Zuge der vertragsgegenständlichen Leistungserbringung kann ein Zugriff auf personenbezogene Daten nicht gänzlich ausgeschlossen werden.

(3) GBS ist verpflichtet, die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich zur Erbringung der in diesem Vertrag vereinbarten Leistungen zu verwenden. GBS ist es gestattet, Duplikats-Dateien zur leistungsgemäßen Erbringung der vereinbarten Leistungen zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

(4) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange GBS für den Auftraggeber die vereinbarten Leistungen erbringt.

§ 2 Weisungen des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) GBS verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen bzw. Aufträge. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Auftraggeber dies anweist.

(3) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von dem Auftraggeber zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn GBS dies verlangt.

(4) Ist GBS der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat GBS den Auftraggeber unverzüglich darauf hinzuweisen.

(5) Empfangsberechtigt für Weisungen beim Auftragsnehmer ist die in Anhang 1 benannte Person.

§ 3 Technische und organisatorische Maßnahmen

(1) GBS verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und zu dokumentieren (Anhang 2). Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. GBS darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss GBS dem Auftraggeber nur wesentliche Anpassungen mitteilen.

(3) GBS unterstützt den Auftraggeber bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. GBS hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Auftraggebers mitzuwirken. GBS wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat dem Auftraggeber alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten von GBS

(1) GBS bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) GBS bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) GBS sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) GBS besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von weiteren Auftragsverarbeiter (Subunternehmer), die in Anlage 3 aufgeführt sind. GBS unterrichtet den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern mindestens 1 Monat im Voraus ausdrücklich in schriftlicher Form und räumt dem Auftraggeber die Möglichkeit ein, gegen derartige Änderungen innerhalb von 1 Monat Einspruch zu erheben. GBS ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. GBS hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieses Vertrages zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus diesem Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat GBS sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutz niveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln) und gem. §4 Abs.9 die vorherige Zustimmung des Auftraggebers eingeholt wurde. Im Falle eines Widerspruchs des Auftraggebers wird der Subunternehmer kein Unterauftragsverarbeiter gegenüber dem Auftraggeber.

(5) GBS verpflichtet sich, alle nach Art. 32 der Datenschutz-Grundverordnung erforderlichen Maßnahmen zu ergreifen.

(6) GBS darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(7) GBS darf die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern sie nicht durch das Recht der Union oder des Mitgliedstaats, dem GBS unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt GBS dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

(8) GBS bestellt einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Dateschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(9) GBS darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(10) GBS unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. GBS benennt einen Ansprechpartner, der den Auftraggeber bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Auftraggeber dessen Kontaktdaten unverzüglich mit. Soweit der Auftraggeber besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntnis erlangung von Daten unterliegt, unterstützt GBS den Auftraggeber hierbei. Auskünfte an die betroffene Person oder Dritte darf GBS nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird GBS dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(11) Wenn zu verarbeitende Daten dem Schutz des § 203 StGB (zur besonderen Verschwiegenheit verpflichteten Berufsgruppen wie Heilberufe, Beratungsberufe, Amtsträger, etc.) unterliegen, obliegt es dem Auftraggeber zu bewerten, welche der zu verarbeitenden Daten dem Schutz von § 203 StGB unterliegen und dies für GBS kenntlich zu machen. Die Kenntlichmachung durch den Auftraggeber erfolgt in Anlage 1 und ggf. durch schriftliche Mitteilung an GBS.

GBS 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.

(12) GBS stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auf traggebers befassten Beschäftigten, andere für GBS tätigen Personen und in Anhang 3 aufgeführten Subunter nehmer, 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 GBS 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 mitwir kende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflich tet wurde.

(13) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet GBS gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Subunternehmers.

(14) Unterauftragsverhältnisse mit Subunternehmern im Sinne dieser Bestimmungen liegen nicht vor, wenn der GBS Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste.

§ 5 Kontrollrechte des Auftraggebers

GBS verpflichtet sich, dass der Auftraggeber oder eine von ihm beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragnehmers zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 6 Mitzuteilende Verstöße von GBS

GBS unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn GBS feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. GBS ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird GBS den Auftraggeber bei der Einhaltung von dessen Meldepflichten unterstützen. Sie wird die Verletzungen des Auftraggebers unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 7 Haftung

Die Haftung von GBS richtet sich nach Artikel 82 der Datenschutz-Grundverordnung, vorbehaltlich folgender Regelungen für Ansprüche des Auftraggebers.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat GBS alle personenbezogenen Daten zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn GBS einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum der Auftraggeber bei GBS durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlag nahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat GBS den Auftrag geber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

(2) Vertragsstrafen sind nicht vereinbart.

(3) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Für den Auftraggeber:

Ort	Datum	Unterschrift / Digitale Signatur:

Für den Auftragnehmer:

Ort, Datum	i.A. Michael Traxler Leiter Service	i.A. Serat Keskin Sachbearbeiter Service
Bayreuth,		

Anhang 1: Auflistung der beauftragten Dienstleistungen, Einzelheiten der Datenverarbeitung und Kontaktdaten des Datenschutzbeauftragten

Produkt	Betriebsart	Gegenstand der Verarbeitung	Dauer der Verarbeitung	Art der personenbezogenen Daten	Kategorien der betroffenen Personen
GBS-Hardware		• Gerätereparaturen • Gerätetausch • Datenrettung von Diktaten • Installation von Soft- und Hardware beim Auftraggeber	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.	Namen, Anschrift, E-Mail-Adresse der Auftraggeber	Auftraggeber der Dienstleistungen und sonstige Vertragspartner des Auftraggebers.
DigtaSoft One DigtaSoft Pro DigtaSoft Speech inkl. dazugehörige Tools zur Geräte-Lizenz- und Benutzerverwaltung Dragon Group (legal & professional)	On premises	• Datenrettung von Diktaten • Installation von Soft- und Hardware beim Auftraggeber • Wartung, Service und Fehlerbehebung in der GBS- und Fremdsoft- und Hardware	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.	Da die originäre Verarbeitung von personenbezogenen Daten bei Nutzung der Produkte on premises nicht Gegenstand der hier betroffenen Aufträge ist, kann GBS grundsätzlich mit jeder Art, auch personenbezogenen Daten besonderer Kategorien (Art. 9 DSGVO), in Berührung kommen. Hierzu können u.a. Namen, Adress- und Bankdaten, Mandantendaten und Gesundheitsdaten aus Krankenakten zählen. Bei allen Produkten werden personenbezogene Daten in der Aufnahme oder dem Transkript Teil der Verarbeitung sein, je nachdem welche personenbezogenen Daten vom Nutzer des Auftraggebers in der Aufnahme bzw. im Transkript erzeugt werden.	Auftraggeber der Dienstleistungen, sowie Kunden, Patienten, Mandanten und sonstige Vertragspartner des Auftraggebers.
	Private Cloud [2]	• Wie On premises zzgl. • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, • Wartung, Konfiguration und Überwachung der Server			
GoSpeech	On premises	• Installation von Soft- und Hardware beim Auftraggeber • Wartung, Service und Fehlerbehebung in der GBS- und Fremdsoft- und Hardware	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt. Die Löschung der erfassten Daten obliegt dem Kunden		
	Private Cloud [1]	• Wie On Premises zzgl. • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, • Wartung, Konfiguration und Überwachung der Server			
	Public Cloud [2]	• Wie On Premises zzgl. • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, • Wartung, Konfiguration und Überwachung der Server			

Anhang 1: Auflistung der beauftragten Dienstleistungen, Einzelheiten der Datenverarbeitung und Kontaktdaten des Datenschutzbeauftragten

Produkt	Betriebsart	Gegenstand der Verarbeitung	Dauer der Verarbeitung	Art der personenbezogenen Daten	Kategorien der betroffenen Personen
GoSpeech Medical Corti	Public Cloud [2]	• Bereitstellung Zugang • Konfiguration von Soft- und Hardware für Auftraggeber • Wartung, Service und Fehlerbehebung • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, • Wartung, Konfiguration und Überwachung der Server	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt. Die Löschung der erfassten Daten obliegt dem Kunden	Da die originäre Verarbeitung von personenbezogenen Daten bei Nutzung der Produkte on premises nicht Gegenstand der hier betroffenen Aufträge ist, kann GBS grundsätzlich mit jeder Art, auch personenbezogenen Daten besonderer Kategorien (Art. 9 DSGVO), in Berührung kommen. Hierzu können u.a. Namen, Adress- und Bankdaten, Mandantendaten und Gesundheitsdaten aus Krankenakten zählen. Bei allen Produkten werden personenbezogene Daten in der Aufnahme oder dem Transkript Teil der Verarbeitung sein, je nachdem welche personenbezogenen Daten vom Nutzer des Auftraggebers in der Aufnahme bzw. im Transkript erzeugt werden.	Auftraggeber der Dienstleistungen, sowie Kunden, Patienten, Mandanten und sonstige Vertragspartner des Auftraggebers.
GoSpeech Medical Translate	On premises	• Installation von Soft- und Hardware beim Auftraggeber • Wartung, Service und Fehlerbehebung in der GBS- und Fremdsoft- und Hardware	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt. Die Löschung der erfassten Übersetzungen erfolgt nach Beendigung des Gesprächs.		
	Private Cloud [1]	• Wie On Premises zzgl. • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, • Wartung, Konfiguration und Überwachung der Server			
	Public Cloud [3]	• Wie On Premises zzgl. • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, Wartung, Konfiguration und Überwachung der Server			
DigtaSoft Speech Direct Dragon Anywhere	On premises	• Installation von Soft- und Hardware beim Auftraggeber • Wartung, Service und Fehlerbehebung in der GBS- und Fremdsoft- und Hardware	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt. Die Löschung der erfassten Daten obliegt dem Kunden		

Anhang 1: Auflistung der beauftragten Dienstleistungen, Einzelheiten der Datenverarbeitung und Kontaktdaten des Datenschutzbeauftragten

Produkt	Betriebsart	Gegenstand der Verarbeitung	Dauer der Verarbeitung	Art der personenbezogenen Daten	Kategorien der betroffenen Personen
	Public Cloud [1]	• Wie On Premises zzgl. • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, Wartung, Konfiguration und Überwachung der Server	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt. Die Löschung der erfassten Daten obliegt dem Kunden	Da die originäre Verarbeitung von personenbezogenen Daten bei Nutzung der Produkte on premises nicht Gegenstand der hier betroffenen Aufträge ist, kann GBS grundsätzlich mit jeder Art, auch personenbezogenen Daten besonderer Kategorien (Art. 9 DSGVO), in Berührung kommen. Hierzu können u.a. Namen, Adress- und Bankdaten, Mandantendaten und Gesundheitsdaten aus Krankenakten zählen. Bei allen Produkten werden personenbezogene Daten in der Aufnahme oder dem Transkript Teil der Verarbeitung sein, je nachdem welche personenbezogenen Daten vom Nutzer des Auftraggebers in der Aufnahme bzw. im Transkript erzeugt werden.	Auftraggeber der Dienstleistungen, sowie Kunden, Patienten, Mandanten und sonstige Vertragspartner des Auftraggebers.
Dragon Copilot	Public Cloud [4]	• Managed Server und Services; • Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, Wartung, Konfiguration und Überwachung der Server	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.		
Dragon Medical One	Public Cloud [4]	• Managed Server und Services; • Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, Wartung, Konfiguration und Überwachung der Server	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.		
Emma RPA	On premises	• Installation von Soft- und Hardware beim Auftraggeber • Wartung, Service und Fehlerbehebung in der GBS- und Fremdsoftware	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.		

Anhang 1: Auflistung der beauftragten Dienstleistungen, Einzelheiten der Datenverarbeitung und Kontaktdaten des Datenschutzbeauftragten

Produkt	Betriebsart	Gegenstand der Verarbeitung	Dauer der Verarbeitung	Art der personenbezogenen Daten	Kategorien der betroffenen Personen
SideKick™	Public Cloud On Premises	Zugriff auf verschiedene KI-Modell mit möglicher Nutzung von NER. Der konkrete Umfang der Verarbeitung hängt von der jeweiligen Nutzung der Plattform durch die Endanwender ab.	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.	Stammdaten (z.B. Namen, Adressen), Kontaktdaten (z.B. E-Mail, Telefon), Nutzungsdaten (z.B. App-Nutzung, Zugriffszeiten), Inhaltsdaten (z.B. vom Nutzer erstellte Inhalte), Technische Daten (z.B. IP-Adressen, Geräteinformationen)	Endnutzer, Kunden, Mitarbeiter
Fluency Direct™	Private Cloud [3]	• Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, Wartung, Konfiguration und Überwachung der Server	Die Daten werden nur zur Erfüllung des Auftrages verarbeitet. Standardmäßig werden Sprachdaten (Audio + Text) für 12 Monate aufbewahrt, um eine optimale Spracherkennungsqualität zu gewährleisten. • Nach den 12 Monaten werde die Textdaten pseudonymisiert und werden zu Entwicklungszwecken 5 Jahre aufbewahrt. • CDI Engage-Daten werden standardmäßig für 2 Jahre aufbewahrt, sofern mit dem Kunden nichts anderes vereinbart wurde. • Daten, die über Citrix ShareFile verarbeitet werden, werden für fünf Tage aufbewahrt. Citrix ShareFile wird verwendet, um einen sicheren Mechanismus zum Austausch von Dateien mit Kunden, wie z. B. Mitarbeiterlisten oder Altdaten, bereitzustellen; es ist nicht als Dateispeicher gedacht. • Alle anderen Daten werden in der Regel für die Dauer des Vertrags oder bis zum ausdrücklichen Wunsch des Kunden sie zu löschen, aufbewahrt.	Da die originäre Verarbeitung von personenbezogenen Daten bei Nutzung der Produkte on premises nicht Gegenstand der hier betroffenen Aufträge ist, kann GBS grundsätzlich mit jeder Art, auch personenbezogenen Daten besonderer Kategorien (Art. 9 DSGVO), in Berührung kommen. Hierzu können u.a. Namen, Adress- und Bankdaten, Mandantendaten und Gesundheitsdaten aus Krankenakten zählen. Bei allen Produkten werden personenbezogene Daten in der Aufnahme oder dem Transkript Teil der Verarbeitung sein, je nachdem welche personenbezogenen Daten vom Nutzer des Auftraggebers in der Aufnahme bzw. im Transkript erzeugt werden	Auftraggeber der Dienstleistungen, sowie Kunden, Patienten, Mandanten und sonstige Vertragspartner des Auftraggebers-Auftraggeber der Dienstleistungen, sowie Kunden, Patienten, Mandanten und sonstige Vertragspartner des Auftraggebers

[1] 23 m GmbH [2] Plusserver GmbH [3] AWS Rechenzentrum in Frankfurt/Main [4] EU Azure Cloud [5] Telecom Cloud

Teile der Daten unterliegen dem Schutz von §203 StGB ◯ Ja ◯ Nein

Anhang 1: Art und Zweck der Verarbeitung

Kenntnis von personenbezogenen Daten nicht ausgeschlossen werden. Bei der Datenrettung werden Diktate wiederhergestellt und gespeichert, bevor sie dem Auftraggeber verschlüsselt zugeschickt werden.

- Bei Technikereinsätzen oder dem Remotezugriff auf die Systeme des Auftraggebers oder im GBS-Rechenzentrum kann der ausführende Mitarbeiter von GBS ggf. Einsicht in personenbezogene Daten bekommen.

- Werden Remotezugriffe mit Einwilligung des Auftraggebers zu Dokumentationszwecken im Rahmen der Gewährleistung aufgezeichnet, können personenbezogene Daten mit der Aufzeichnung abgespeichert werden.

- Corti, GoSpeech Medical, MediSync: Die Daten werden zur Erstellung von medizinischen Dokumentationen verarbeitet, die Modelle verarbeiten Audiodateien und andere Daten als Eingabe, um eine Ausgabe zu erstellen.

- Medisync nutzt die Open Telekom Cloud (Private Cloud) in Biere und Magdeburg (Sachsen-Anhalt) und die AWS-Cloud (Public Cloud) in Frankfurt/Main. Audiodateien werden vom AI-Modell verarbeitet, aber nicht manipuliert. Während der Nutzung verarbeiten die AI-Modelle mit vollständig nicht anonymisierten Eingabedaten. Sprachaufzeichnungen und Transkriptionen und Kundendaten werden ausschließlich zur Zweckerfüllung eingesetzt und nicht zum Training von KI-Lösungen oder Verbesserung von Sprachmodellen genutzt.

- Corti nutzt eine Microsoft Azure-Infrastruktur in den drei Hauptregionen in der Europäischen Union (NL, IR, DK). Audiodateien werden vom AI-Modell verarbeitet, aber nicht manipuliert. Während der Nutzung verarbeiten Corti AI-Modelle mit vollständig nicht anonymisierten Eingabedaten. Sprachaufzeichnungen und Transkriptionen und Kundendaten werden ausschließlich zur Zweckerfüllung eingesetzt und nicht zum Training von KI-Lösungen oder Verbesserung von Sprachmodellen genutzt.

- Dragon Copilot und Dragon Medical One nutzt die Microsoft Azure-Infrastruktur in den Hauptregionen in der Europäischen Union (NL, IR, DE). Audiodateien werden vom AI-Modell verarbeitet, aber nicht manipuliert. Während der Nutzung verarbeiten die AI-Modelle mit vollständig nicht anonymisierten Eingabedaten. Sprachaufzeichnungen und Transkriptionen und Kundendaten werden ausschließlich zur Zweckerfüllung eingesetzt und nicht zum Training von KI-Lösungen oder Verbesserung von Sprachmodellen genutzt.

- SideKick™ stelltbereit und betreibt eine KI-gestützten Plattform zur Verarbeitung von Nutzeranfragen und Unternehmensdaten, zur Generierung von Antworten und Analysen, zur Unterstützung von Geschäftsprozessen sowie zur Automatisierung von Arbeitsabläufen durch KI-Modelle und intelligente Agents. In der Betriebsform Public Cloud werden ausschließlich Rechenzentren in Deutschland verwendet.

- Fluency Direct™: Benutzereinstellungen, Benutzerprofile, Sprachdateien und Dokumente werden in der Cloud gehostet, ausschließlich in der AWS in Frankfurt Main, in redundanten Rechenzentren. Alle an Solventum-Ressourcen gesendeten Informationen werden sicher mit TLS1.2 übertragen, einem verschlüsselten Übertragungsmechanismus nach Industriestandard. Innerhalb von TLS1.2 verwenden wir AES 256-Bit-Verschlüsselung (High) und RSA mit 2048-Bit-Austausch. Solventum-Ressourcen kommunizieren über Port 443 und 8077.
  - Standardmäßig werden Sprachdaten (Audio + Text) für 12 Monate aufbewahrt, um eine optimale Spracherkennungsqualität zu gewährleisten.
  - Nach den 12 Monaten werde die Textdaten pseudonymisiert und werden zu Entwicklungszwecken 5 Jahre aufbewahrt.
  - CDI Engage-Daten werden standardmäßig für 2 Jahre aufbewahrt, sofern mit dem Kunden nichts anderes vereinbart wurde.
  - Daten, die über Citrix ShareFile verarbeitet werden, werden für fünf Tage aufbewahrt. Citrix ShareFile wird verwendet, um einen sicheren Mechanismus zum Austausch von Dateien mit Kunden, wie z. B. Mitarbeiterlisten oder Altdaten, bereitzustellen; es ist nicht als Dateispeicher gedacht.
  - Alle anderen Daten werden in der Regel für die Dauer des Vertrags oder bis zum ausdrücklichen Wunsch des Kunden sie zu löschen, aufbewahrt.

Anhang 1: Art und Zweck der Verarbeitung

Datenschutzbeauftragter und Weisungsberechtigter	
Name und Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers	Armin Schymala datenschutzbeauftragter@grundig-gbs.com Am Schlag 39 93138 Lappersdorf Telefon: +49 (0) 941 29 84 868 Mobil: +49 (0) 151 50 036 105
Name und Kontaktdaten des Weisungsberechtigten des Auftragnehmers	Michael Traxler michael.traxler@grundig-gbs.com Weiherstrasse 10 95448 Bayreuth

Anhang 2: Technische und organisatorische Maßnahmen zum Erhalt des Datenschutzes bei der Grundig Business Systems GmbH & Co. KG

Inhaltsverzeichnis

Anhang 2: Technische und organisatorische Maßnahmen zum Erhalt des Datenschutzes bei der Grundig Business Systems GmbH & Co. KG	9
1.1. Zutrittskontrolle	10
1.2. Zugangskontrolle	10
1.3. Zugriffskontrolle	11
1.4. Trennungskontrolle	11
2. Integrität	12
2.1. Weitergabekontrolle	12
2.2. Eingangskontrolle	12
3. Verfügbarkeit und Belastbarkeit	13
3.1. Verfügbarkeitskontrolle	13
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	13
4.1. Datenschutz-Maßnahmen	13
4.2. Incident-Response-Management	14
4.3. Auftragskontrolle (Outsourcing an Dritte)	14
Anhang 3: Subunternehmen	15

Stand 30.07.2025

Technische und organisatorische Maßnahmen zum Erhalt des Datenschutzes bei der Grundig Business Systems GmbH & Co. KG

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Trannsponder, Kontrollen des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisungen, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung / Liste
Sicherheitsschlösser / RFID-Chips	Besucherbuch
Automatisches Zugangskontrollsystem	Besucher nur in Begleitung von Mitarbeitern
Teilweise Klimaanlagen	Sorgfalt bei der Auswahl des Reinigungspersonals
Videoüberwachung der Eingänge	Besetzter Empfang / Rezeption
Bewegungsmelder	Externer Wachdienst
Netzwerkverteiler abgeschlossen	
Serverraum abgeschlossen	

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswörter, Benutzerkennungen mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von Call-Back-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
Multifaktor Authentifizierung	Verwaltung von Benutzerberechtigungen
Anti-Viren-Software Server	Erstellen von Benutzerprofilen
Anti-Virus-Software Clients	Zentrale und einheitliche Passwortvergabe
Hardware Firewall	Richtlinie „Sicheres Passwort“
Software Firewall	Richtlinie Mobiles Arbeiten
Verschlüsselung von Datenträgern in Notebooks	
Conditional Access Richtline	

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten aus schließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle wird unter anderem durchgeeignete Berechtigungskonzepte gewährleistet, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes und Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder	Einsatz von Berechtigungskonzepten
Physische Löschung von Datenträgern	Minimale Anzahl an Administrationen
Zugriffskontrolle auf Verwendungen, bei der Eingabe und Löschung von Daten	Verwaltung der Benutzerrechte durch Administration
Passwortrichtlinie inkl. Passwortlänge und -wechsel	Anzahl der lokalen Administratoren auf das Nötigste beschränkt
Automatisches Bildschirm Timeout	
Absperren der Büros im Personalbereich bei Verlassen	

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Physikalische Trennung von Systemen, Datenbanken und Datenträgern	Steuerung über Berechtigungsstruktur
Mandantenfähigkeit relevanter Anwendungen	Festsetzung von Datenbankrechten
Zugriffskontrolle auf Verwendungen bei der Eingabe und Löschung von Daten	Datensätze sind tlw. mit Zweckattributen versehen
Trennung von Produktiv- und Testsystem	

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind z. B. Transportbehälter mit Schließvorrichtungen und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
Datenverkehr grundsätzlich SSL verschlüsselt	Persönliche Übergabe mit Protokollen
Protokollierung der Zugriffe	Übersicht regelmäßiger Abruf- und Vermittlungsvorgängen
Tlw. Nutzung von Signaturverfahren	
Klassifizierung	

2.2 Eingangskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe sowie Änderung und Löschung von Daten	Rechtevergabe zur Eingabe, Änderung und Löschung von Daten (Berechtigungskonzept)
Automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung sowie Löschung von Daten durch individuelle Benutzernamen durch das IT- System
Data-loss Prevention Richtlinie	Übersicht sowie Dokumentation, mit welchen Programmen Daten eingegeben, geändert bzw. gelöscht werden können
	Eindeutige Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Backup- und Recovery-Konzept
Feuerlöscher in den Rechenzentren und auf den Gängen der Büros	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung – Temperatur und Feuchtigkeit (Rechenzentren)	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Unterbrechungsfreie Stromversorgung (USV) für die Server /und Netzwerkkomponenten	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
Klimaanlage in den Serverräumen	Existenz eines Notfallplans
	Serveraum im ersten Stock (Hochwasser)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
Wirksamkeitsprüfung der technischen Schutzmaß-nahmen werden mindestens einmal pro Jahr durchgeführt	Externer Datenschutzbeauftragter
Manuell gepflegtes Sicherheitskonzept	Schulung von Mitarbeitern
	Regelmäßige Sensibilisierung der Mitarbeiter
	Interner Ansprechpartner für den Datenschutz (zusätzlich zum Datenschutzbeauftragten)
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen ist vorhanden
	Löschkonzept

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen:

Technische Maßnahmen	Organisatorische Maßnahmen
Firewall-Einsatz und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Datenschutzvorfällen
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Datenschutzvorfällen
Einsatz von Virenscanner und regelmäßige Aktualisierung	Einbindung des Datenschutzbeauftragten bei Datenschutzvorfällen
	Dokumentation von Datenschutzvorfällen durch Ticket-system

4.3. Auftragskontrolle (Outsourcing an Dritte, Subunternehmen)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Falls Subunternehmer eingesetzt werden, sind folgende organisatorische Maßnahmen getroffen:

- Vorherige Prüfung der getroffenen Sicherheitsmaßnahmen
- Lieferantenaudits gem., ISO 9001 und ISO 27001
- Auswahl des Auftragnehmers erfolgt unter Sorgfaltsgesichtspunkten
- Abschluss der erforderlichen Verträge (AVV)
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Auftragsbeendigung
- Regelmäßige Überprüfung des Auftragnehmers im Hinblick auf sein Schutzniveau

Anhang 3:

Subunternehmen

Subunternehmen	Beschreibung	Anmerkung
Teccle motion GmbH Hanauer Landstraße 182a 60314 Frankfurt am Main	IT-Dienstleister	
SaM Solutions GmbH Römerstraße 32 82205 Gilching	Software Engineering	
Hippolyt Thum GmbH Gummistr. 21 95326 Kulmbach	IT Dienstleister für Drucker und Scanner	
IFE GmbH Podbielskistrasse 269 30655 Hannover	Rechenzentrums- und ERP- Systembetreuung	
envisia GmbH Salzmatten 23 79341 Kenzingen	Dokumentenarchivierung und -versionskontrolle	
Plusserver GmbH Venloer Straße 47 50672 Köln	Rechenzentrums- und Wartungsdienstleistungen	Nur für GoSpeech SaaS-Nutzung
23 Media GmbH Johann-Krane-Weg 18 48149 Münster	Rechenzentrums- und Wartungsdienstleistungen	
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Fernwartungssoftware	
Nuance Communications Ireland Limited 20 Merrion Road, Ballsbridge Dublin 4 Irland	Rechenzentrums- und Wartungsdienstleistung, Betrieb von Spracherkennungsserver	Nur für Dragon Medical One
GBS electronic solution GmbH Weiherstrasse 10 95448 Bayreuth	Reparatur von GBS Hardware	
WIANCO OTT Robotics GmbH Schlosspark 1 64342 Seeheim-Jugenheim	RPA Technologie	Nur für Emma
Mabel AI AB c/o Sahlgrenska Science Park, Medicinaregatan 8A, 41390, Gothenburg, Sweden	Medizinische Übersetzungen	Nur für Mabel AI / GoSpeech Medical Translate
ALVAO s.r.o. Hlohová 1455/10 591 01 Žďár nad Sázavou Czech Republic	Internes Asset-Management von GBS	
Corti ApS Kuglegårdsvej 2, 2 sal, 1434, Copenhagen K, Denmark	Medizinische Dokumentation	Nur für Corti Assistant und GoSpeech Medical
MediSync GmbH Wormser Strasse 47 50677 Köln	Medizinische Dokumentation	Nur für MediSync

Anhang 3:

Subunternehmen

Subunternehmen	Beschreibung	Anmerkung
Cantab Research Limited (Speechmatics) Unit 296, Cambridge Science Park, Milton Road, Cambridge CB4 0WD, UK	Transkriptionsengine	Nur für GoSpeech
ORdigiNAL B.V. Transistorstraat 31 NL-1322 CK ALMERE	Lizenzen und Support	Für Dragon Medical One, Dragon Anywhere und Dragon Group und Dragon Copilot
Tobit Software GmbH Parallelstraße 41 48683 Ahaus	Unified Agentic AI Ecossystem	Für SideKick™
Solventum Germany GmbH Edisonstraße 6 59174 Kamen	Rechenzentrums- und Wartungs-dienstleistung, Betrieb von Sprach-erkennungsserver	Nur für Fluency