Auftragsverarbeitungsvertrag

gem. Art. 28 Datenschutzgrundverordnung (EU) 2016/679 (DSGVO)

Bereitstellung eines KI-Telefonassistenten und/oder KI-Online Rezeption

für medizinische Praxen

zwischen

Kunde

(Auftraggeber)

und

CompuGroup Medical Deutschland AG
Maria Trost 21
56070 Koblenz
(Auftragnehmer, CGM)

Präambel

Der Auftragnehmer, die CompuGroup Medical Deutschland AG (nachfolgend: CGM), geschäftsansässig in Maria Trost 21, 56070 Koblenz, Deutschland, im Handelsregister des Amtsgerichts Koblenz unter der Nummer HRB 22901 registriert, ist einer der führenden IT-Dienstleister im Gesundheitssektor. CGM bietet Gesundheitsdienstleistern als Ergänzung zu deren Praxisverwaltungssoftware (a) eine KI-gestützte Software-Anwendung, die patientenbezogene Anfragen per Telefon in Form einer audiobasierten Real-Time Konversation automatisch bearbeitet (der KI-Telefonassistent) sowie (b) als Ergänzung zu deren Praxisverwaltungssoftware eine KI-gestützte Software-Anwendung, die patientenbezogene Anfragen über ein Widget auf der Praxis Homepage in Echtzeit automatisiert verarbeitet (die KI-Online Rezeption).

Der KI-Telefonassistent soll zukünftig als unterstützendes System zur Verbesserung der Effizienz administrativer und kommunikativer Prozesse in medizinischen Einrichtungen wie Arztpraxen dienen. Er automatisiert die Bearbeitung von telefonischen Anfragen und extrahiert relevante Informationen für administrative Zwecke, einschließlich der Weiterleitung von Nachrichten und der Terminverwaltung.

Die KI-Online Rezeption dient als unterstützendes System zur Verbesserung der Effizienz administrativer und kommunikativer Prozesse in medizinischen Einrichtungen wie Arztpraxen. Sie automatisiert die Bearbeitung digitaler Anfragen und extrahiert relevante Informationen für administrative Zwecke, einschließlich der Weiterleitung von Nachrichten und der Unterstützung bei der Terminverwaltung.

Dieser Vertrag regelt entsprechend der vertraglich vereinbarten Leistungen die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der Nutzung des KI-Telefonassistenten und/oder der KI-Online Rezeption für medizinische Praxen (zusammen gemeinsam oder jeweils einzeln „Software"), die von CompuGroup Medical Deutschland AG vermittelt und über die Azure-Dienste bereitgestellt wird.

Dem Auftraggeber wird mit Bestätigung der Teilnahmebedingungen das Recht eingeräumt, den KI-Telefonassistenten und/oder die KI-Online Rezeption zu nutzen.

§ 1 Gegenstand, Umfang, Art und Zweck

1.1 Dieser Vertrag regelt die Auftragsverarbeitung im Rahmen der Leistungen, die zwischen dem Auftraggeber und dem Auftragnehmer vereinbart sind und/oder werden und in **Anlage 1** als Gegenstand der Auftragsverarbeitung gelistet sind. Die **Anlage 1** wird während der Laufzeit dieses Vertrages jeweils einvernehmlich zwischen den Parteien unter Einhaltung des Formerfordernisses gem. § 10.1 aktualisiert.

1.2 Umfang, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zum jeweiligen Gegenstand gem. § 1.1 gelistet.

1.3 Die Verarbeitung personenbezogener Daten unter diesem Vertrag erfolgt in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Eine Verarbeitung durch Subauftragnehmer in einem Drittland richtet sich nach § 6 in Verbindung mit Anlage 1 dieses Auftragsverarbeitungsvertrages. Jede Verlagerung in ein Drittland (nicht EU-/EWR-Staat) darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Dies gilt auch für die Datenverarbeitung durch den Unterauftragnehmer für elektronische Kommunikationsdienste nach Ziffer 8 dieses Vertrages, der eine Verarbeitung personenbezogener Daten außerhalb des EWR nur in Übereinstimmung mit den verbindlichen internen Datenschutzvorschriften (sog. Binding Corporate Rules) und dem EU-US Datenschutzrahmenabkommen (sog. Data Privacy Framework) sowie weiteren geeigneten Sicherheitsmaßnahmen vornehmen darf.

§ 2 Laufzeit

2.1 Dieser Vertrag läuft, solange der Auftragnehmer gegenüber dem Auftraggeber Leistungen erbringt, die Gegenstand der Auftragsverarbeitung gem. § 1.1 sind. Er endet automatisch, ohne dass es einer Kündigung bedarf, sobald der Auftragnehmer endgültig keine Leistungen mehr als Gegenstand der Auftragsverarbeitung nach § 1.1 erbringt, d.h. die Laufzeit entspricht der Zeit der Bereitstellung des KI-Telefonassistenten. Haben die Parteien nach den Teilnahmebedingungen der Pilotphase, deren Leistungen Gegenstand dieses Auftragsverarbeitungsvertrages sind, eine befristete Leistungserbringung und ein Auflösungsdatum vereinbart, so endet dieser Auftragsverarbeitungsvertrag auch mit dem Ablauf dieses Datums, ohne das es einer Kündigung bedarf. Der Auftragnehmer hat die Verarbeitung personenbezogener Daten in diesem Falle mit dem Ablaufdatum einzustellen. Dasselbe gilt mit dem Beendigungsdatum der Teilnahmebedingungen, wenn diese wirksam ordentlich oder außerordentlich gekündigt wurde.

2.2 Die Parteien können diesen Vertrag jederzeit außerordentlich ohne Einhaltung einer Frist aus wichtigem Grund ganz oder teilweise in Bezug auf einen Gegenstand nach § 1.1 kündigen.

2.2.1 Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn der Auftragnehmer schwerwiegend gegen das anwendbare Datenschutzrecht verstößt und diesen Verstoß nicht innerhalb angemessener Frist nach Aufforderung durch den Auftraggeber abstellt.

2.2.2 Ein wichtiger Grund liegt für den Auftragnehmern insbesondere vor, wenn eine Weisung des Auftraggebers nach Ansicht des Auftragnehmers gegen das anwendbare Datenschutzrecht verstößt, der Auftragnehmer dies dem Auftraggeber gem. § 8.5 mitgeteilt hat und der Auftraggeber dennoch auf Durchführung seiner Weisung besteht.

2.3 Nach Beendigung des Vertrags löscht der Auftragnehmer innerhalb angemessener Frist alle im Auftrag unter diesem Vertrag verarbeiteten personenbezogenen Daten oder gibt diese an den Auftraggeber zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Trifft der Auftraggeber bis zum Zeitpunkt des Vertragsendes eine Wahl nach Satz 1 und unterrichtet den Auftragnehmer darüber, ist der Auftragnehmer an diese gebunden. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragnehmer weiterhin die Einhaltung dieser Klauseln. Die vorstehenden Regelungen dieses § 2.3 gelten entsprechend, wenn der Vertrag teilweise in Bezug auf einen Gegenstand nach § 1.1 endet.

§ 3 Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer stellt ein dem Risiko angemessenes Schutzniveau der Datenverarbeitung gem. Art. 28 Abs. 3 lit. c, 32 DSGVO sicher. Die zum Zeitpunkt des Vertragsschlusses hierzu

vereinbarten technischen und organisatorischen Maßnahmen sind diesem Vertrag als **Anlage 2a und 2b** beigefügt.

3.2 Es steht dem Auftragnehmer frei, mobiles Arbeiten auch für unter diesem Vertrag im Auftrag verarbeitete Daten vorzusehen, soweit und solange er auch in diesen Fällen ein angemessenes Schutzniveau der Datenverarbeitung gem. Art. 28 Abs. 3 lit. c, 32 DSGVO sicherstellt.

3.3 Die technischen und organisatorischen Maßnahmen der Software unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, zu den in **Anlage 2a und 2b** vereinbarten Maßnahmen alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau bei Vertragsschluss festgelegten Maßnahmen nicht wesentlich unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf dessen Anfrage hin mitzuteilen.

§ 4 Betroffenenrechte und Zusammenarbeit

4.1 Der Auftraggeber ist verantwortlich für die Erfüllung von Betroffenenrechten nach Art. 12 ff. DSGVO. Soweit sich eine von der Datenverarbeitung unter diesem Vertrag betroffene Person unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Der Auftraggeber unterrichtet den Auftragnehmer unverzüglich über alle Unregelmäßigkeiten der Ergebnisse der vom Auftragnehmer im Auftrag verarbeiteten Daten.

4.3 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Verletzungen personenbezogener Daten gem. Art. 33 Abs. 2 DSGVO und übermittelt dem Auftraggeber alle ihm vorliegenden Informationen, die für eine etwaige Meldung nach Art. 33, 34 DSGVO erforderlich sind.

4.4 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der datenschutzrechtlichen Anforderungen, insbesondere

a) bei der Sicherstellung der Erfüllbarkeit und der Erfüllung von Betroffenenrechten;

b) bei der Umsetzung der Anforderungen an die Sicherheit der Datenverarbeitung nach Art. 32 DSGVO durch den Auftraggeber;

c) bei einer erforderlichen Folgenabschätzung nach Art. 35, 36 DSGVO;

d) im Fall einer Verletzung des Schutzes personenbezogener Daten bei der Erfüllung der Pflichten nach Art. 33, 34 DSGVO.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer erfüllt die ihm aus dem jeweils anwendbaren Datenschutzrecht obliegenden Pflichten, insbesondere jene gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet der Auftragnehmer insbesondere die Einhaltung folgender Vorgaben:

a) Die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers sind in **Anlage 3** genannt. Im Fall von Änderungen in der Person oder den Kontaktdaten des Datenschutzbeauftragten wird der Auftragnehmer den Auftraggeber von der Änderung in Kenntnis setzen.

b) Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO und etwaiger anwendbarer Spezialvorschriften, etwa § 203 StGB. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

c) Der Auftragnehmer und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der dokumentierten Weisung vom Auftraggeber verarbeiten unter Berücksichtigung der Pflichten und Befugnisse dieses Vertrages, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

§ 6 Unterauftragsverhältnisse

6.1 Der Auftragnehmer ist berechtigt, zur Ausführung von Aufträgen und Teilen von Aufträgen unter diesem Vertrag Subunternehmer unter Beachtung der Bestimmungen in diesem § 6 einzusetzen. Die zum Zeitpunkt des Vertragsschlusses berechtigt eingesetzten Subunternehmer sind in **Anlage 1, Nr.5** aufgeführt.

6.2 Beabsichtigt der Auftragnehmer, neue Subunternehmen einzusetzen oder bestehende Subunternehmer zu ersetzen, unterrichtet der den Auftraggeber darüber im Voraus in Textform. Der Auftraggeber ist berechtigt, dem Einsatz neuer Subunternehmer oder dem Ersatz bestehender Subunternehmer innerhalb von drei Wochen nach Bekanntgabe der Information nach Satz 1 aus nachweislich wichtigen datenschutzrechtlichen Gründen zu widersprechen. Geht beim Auftragnehmer kein Widerspruch innerhalb der Frist ein, gilt der neue Subunternehmer als genehmigt. Geht ein Widerspruch innerhalb der Frist ein, werden sich die Parteien um eine

einvernehmliche Lösung bemühen. Sofern keine einvernehmliche Lösung gefunden wird, steht dem Auftragnehmer ein außerordentliches Kündigungsrecht hinsichtlich des unter diesem Vertrag betroffenen Gegenstands einschließlich des zugehörigen Hauptvertrags zu.

6.3 Der Auftragnehmer hat vertraglich gegenüber dem Subunternehmer sicherzustellen, dass die in diesem Vertrag und in sonstigen Vereinbarungen festgelegten Pflichten und rechtlichen Grenzen auch gegenüber dem jeweiligen Subunternehmer gelten. Der Auftragnehmer stellt dem Auftraggeber auf dessen Verlangen eine Kopie seiner Auftragsverarbeitungsvereinbarung mit dem Subunternehmer und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragnehmer den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie insofern in Teilen unkenntlich machen. Die Weiterleitung der Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach diesem § 6 erfüllt.

6.4 Ein Unterauftragsverhältnis nach diesem § 6 liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind, insbesondere, aber nicht abschließend, Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen und Bewachungsdienste.

§ 7 Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer bearbeitet Anfragen des Auftraggebers bezüglich der Verarbeitung von Daten gemäß diesem Vertrag umgehend und in angemessener Weise.

7.2 Der Auftraggeber hat das Recht, zur Einhaltung dieses Vertrages und der Pflichten vom Auftragnehmer nach Art. 28 DSGVO erforderliche Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Die Überprüfungen erfolgen vorrangig durch die Überlassung geeigneter Informationen auf Anforderung des Auftraggebers. Der Auftragnehmer erteilt dem Auftraggeber dazu auf Anforderung die erforderlichen Auskünfte und weist die Einhaltung der Anforderungen dieses Vertrages und des Art. 28 DSGVO nach. Der Auftragnehmer ist berechtigt, den Nachweis durch geeignete Zertifizierungen zu führen. Nachrangig sind im Einzelfall auch vor Ort Inspektionen im Geschäftsbetrieb des Auftragnehmers zulässig, soweit diese zur Überprüfung nach Satz 1 unabdingbar sind, in der Regel nur in angemessenen Abständen, zu den üblichen Geschäftszeiten, nach vorheriger Anmeldung mit angemessener Vorlaufzeit und ohne wesentliche Störung des Betriebsablaufs. Überprüfungen vor Ort kann der Auftragnehmer von der Unterzeichnung angemessener Verschwiegenheitserklärungen abhängig machen; sollte ein vom Auftraggeber beauftragter Prüfer in einem Wettbewerbsverhältnis mit dem Auftragnehmer stellen, darf der Auftragnehmer dem Einsatz dieses Prüfers widersprechen.

§ 8 Weisungsbefugnis des Auftraggebers

8.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich gemäß den in diesem Vertrag getroffenen Festlegungen und den Weisungen vom Auftraggeber, es sei denn er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

8.2 Der Auftragnehmer verfolgt bei der Verarbeitung keine anderen und insbesondere keine eigenen, über die Vertragsdurchführung hinausgehenden Zwecke, es sei denn, er oder einer seiner Unterauftragnehmer führt Verarbeitungen gemäß der nachfolgenden Ziffern dieses Vertrages durch. Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen getrennt verarbeitet werden.

8.3 Der Auftraggeber erteilt dem Auftragnehmer Weisungen, wie und in welchem Umfang die Daten verarbeitet werden dürfen. Weisungen vom Auftraggeber werden mit diesem Vertrag oder im Einzelfall durch vom Auftraggeber benannte (oder nach der Verkehrsanschauung als befugt geltende) weisungsberechtigte Personen an einen oder mehrere vom Auftragnehmer benannte (oder nach der Verkehrsanschauung als befugt geltende) Weisungsempfänger unter Einhaltung des Formerfordernisses gem. § 10.1 erteilt.

8.4 Weisungen unterliegen dem Formerfordernisses gem. § 10.1; mündlich erteilte Weisungen sind unverzüglich entsprechend zu bestätigen. Die Bestätigung der mündlichen Weisungen sowie Weisungen, die außerhalb dieses Vertrages dem Hauptvertrag getroffen wurden/werden, sind vom Auftraggeber jeweils zusammen mit diesem Vertrag so aufzubewahren, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.

8.5 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen das anwendbare Datenschutzrecht verstößt. Der Auftragnehmer ist in diesem Fall berechtigt, die Verarbeitung auszusetzen, bis der Auftraggeber ihm eine anderweitige Weisung erteilt; dies umfasst auch eine Befreiung von der entsprechenden hauptvertraglichen Leistungspflicht des Auftragnehmers, nicht aber von Gegenleistungspflichten des Auftraggebers; § 2.2.2 bleibt unberührt.

8.6 Zur Validierung der Qualität der im Produkt bereitgestellten KI-Systeme im Interesse des Auftraggebers, konkret im Zusammenhang mit dessen freiwilliger Teilnahme an der Pilotierung neuer Funktionalitäten des Produkts oder im Rahmen von Supportanfragen, kann der Auftragnehmer auf zuvor anonymisierte Datensätze zu Chats und Telefongesprächen zugreifen. Die Verarbeitung dieser Datensätze erfolgt ausschließlich auf hierfür vorgesehenen eigenen Instanzen, wobei der Zugriff auf einen festgelegten Personenkreis beschränkt ist. Durch die vor-

geschaltete Anonymisierung ist sichergestellt, dass die verwendeten Daten keine Rückschlüsse auf individuelle Betroffene zulassen; eine Zuordnung ist ausschließlich zur jeweiligen Praxis möglich. Zudem ist der Auftragnehmer in eigener Verantwortlichkeit zwecks Erfüllung rechtlicher Verpflichtungen im Einklang mit dem europäischen Rechtsrahmen zur Datenverarbeitung berechtigt (vergleiche § 8.1).

8.7 Zur Bearbeitung von durch den Auftraggeber mittels entsprechender Produktfunktionen ausgelösten Supportanfragen (z. B. über eine Funktion „Problem melden“) kann der Auftragnehmer auf die jeweils betroffenen Nutzungsvorgänge der Software einschließlich der hierbei anfallenden Inhalte und Metadaten zugreifen. Die Übermittlung dieser Daten an den Auftragnehmer erfolgt bei durch den Auftraggeber initiierten Anfragen jeweils erst nach bewusster Auslösung und Bestätigung des Absendevorgangs. Der Auftragnehmer ist berechtigt, diese Daten zwecks Analyse und Behebung von Störungen sowie der damit einhergehenden Qualitätssicherung und Verbesserung der betroffenen Funktionalitäten der Software und zugrunde liegender Systeme, nach Möglichkeit unter Einsatz von Anonymisierung oder Pseudonymisierung, zu verarbeiten und hierfür mit einschlägigen technischen Protokolldaten zu verknüpfen. Nach Abschluss der hierfür erforderlichen Maßnahmen werden die im Rahmen der jeweiligen Supportanfrage übermittelten Daten unverzüglich gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

8.8 Unabhängig von diesem § 8 ist ein für die Erbringung der durch die Software vorausgesetzten elektronischen Telekommunikationsdienste eingesetzter Unterauftragnehmer in getrennter Verantwortlichkeit befugt, bestimmte personenbezogene Daten nach der Anlage 1 im erforderlichen und rechtmäßigen Umfang zu den folgenden Zwecken zu verarbeiten: (a) unter ausschließlicher Verwendung von Telekommunikationsmetadaten die notwendigen Aufgaben als Anbieter elektronischer Telekommunikationsdienste zu erfüllen, einschließlich der Verarbeitung dieser Daten für Abrechnungs-, Steuer-, Rechnungs-, Prüfungs- und Compliance-Zwecke, zur Bereitzustellung, Fortentwicklung und Sicherstellung dieser Dienste sowie zur Verhinderung, Feststellung und Ermittlung von Sicherheitsvorfällen und zur Verwaltung der Sicherheitsvorkehrungen; (b) Missbrauch der elektronischen Telekommunikationsdienste zu verhindern, zu erkennen oder zu untersuchen, einschließlich Spam, betrügerischen Aktivitäten und Verstößen gegen die Sicherheitsrichtlinien des Anbieters, oder um Telekommunikationsnetzanbietern, Aufsichtsbehörden oder Strafverfolgungsbehörden bei der Bekämpfung von Spam oder betrügerischen Aktivitäten zu unterstützen; (c) unter ausschließlicher Verwendung von Telekommunikationsmetadaten Produkte und Dienste im Kontext der genutzten elektronischen Kommunikationsdienste zu entwickeln und zu verbessern sowie die Leistung, Funktionalität und Sicherheit dieser Dienste zu verbessern; (d) die rechtlichen und regulatorischen Verpflichtungen zu erfüllen, einschließlich vorgeschriebener Aufzeichnungen und Einhaltung von Vorschriften der Telekommunikationsbranche und vertraglicher Verpflichtungen gegenüber anderen Telekommunikationsanbietern. Der Unterauftragnehmer wird dabei in allen vorgenannten Fällen geeignete Maßnahmen anwenden, um personenbezogene Daten, die für die vorgenannten Zwecke verwendet werden, zu minimieren, anonymisieren, insbesondere im Fall von Gesundheitsdaten, oder zu pseudonymisieren, sodass betroffene Person

nicht identifiziert werden können. Der Unterauftragnehmer wird keine Re-Identifizierung der vormals personenbezogenen Daten unternehmen.

§ 9 Haftung

9.1 Die Haftung der Parteien gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO.

9.2 Im Innenverhältnis haften die Parteien für Vorsatz und grobe Fahrlässigkeit nach den gesetzlichen Vorschriften. Das gleiche gilt bei schuldhaft verursachten Schäden aus der Verletzung des Lebens, des Körpers, der Gesundheit oder der Verletzung von Produkthaftungspflichten sowie im Falle arglistig verschwiegener Mängel.

9.3 Im Übrigen ist die Haftung des Auftragnehmers im Innenverhältnis beschränkt auf die Verletzung von Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglichen und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf (Kardinalspflichten). Die Haftung des Auftragnehmers im Innenverhältnis ist im Fall der leicht fahrlässigen Verletzung von Kardinalspflichten der Höhe nach begrenzt auf den vertragstypisch vorhersehbaren Schaden. Für Schäden, die auf leichter Fahrlässigkeit und nicht auf Verletzung des Lebens, des Körpers, der Gesundheit, der Verletzung von Produkthaftungspflichten oder von Kardinalspflichten beruhen, ist der Schadensersatzanspruch des Auftraggebers gegen den Auftragnehmer auf das Zweifache Vertragsvolumen des Hauptvertrages in einem Kalenderjahr begrenzt. Die Haftungsbegrenzungen aus Punkt 9.2 gilt vorrangig gegenüberetwaigen Haftungsbegrenzungen im hauptvertrag oder allgemeinen Geschäftsbedingungen der Parteien.

§ 10 Schlussbestimmungen

10.1 Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform (einschließlich elektronisch signierter Textform, z.B. mittels DocuSign). Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.2 Die Regelungen dieses Vertrages gehen im Zweifel den Regelungen des Hauptvertrages vor.

10.3 Sollten sich einzelne Bestimmungen dieses Vertrages ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame oder durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

10.4 Dieser Vertrag unterliegt deutschem Recht (einschließlich der Datenschutzgrundverordnung). Ausschließlicher Gerichtsstand ist Koblenz.

Anlage 1 – Gegenstand der Auftragsverarbeitung

1. Gegenstand

Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung der unter Punkt 2 genannten Aufgaben durch den Auftragnehmer im Kontext der gemäß Hauptvertrag durch den Kunden bezogenen und durch den Auftragnehmer bereitgestellten Software:

- Bereitstellung des KI-Telefonassistenten für medizinische Praxen; und/oder
- Bereitstellung der KI-Online Rezeption für medizinische Praxen

2. Umfang, Art, Zweck der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben und umfasst insbesondere folgende Leistungen:

a. KI-Telefonassistent:

Der KI-Telefonassistent ist eine KI-gestützte Software-Anwendung, die eingehende Telefonanfragen in Echtzeit transkribiert. Dabei werden die wesentlichen Informationen der Anrufe extrahiert und strukturiert zusammengefasst, sodass das Praxisteam das Anliegen der Anrufer effizient erfassen und weiterbearbeiten kann. Der KI-Telefonassistent nutzt diese transkribierten Informationen zudem, um mittels eines Large Language Models unter Nutzung von Wahrscheinlichkeitsaussagen Antworten zu generieren und ein Gespräch in Echtzeit mit dem Anrufenden zu führen. Dies dient dem Zweck, die Anfrage, etwa in Form einer Terminvereinbarung oder eines Rückrufs zu beantworten.

Sofern der Auftraggeber Funktionen zur Terminvereinbarung oder vergleichbaren administrativen Prozessen der CGM-Gruppe (z. B. CLICKDOC) aktiviert und nutzt, erfolgt zur Durchführung dieser Funktionen ein temporärer Datenaustausch mit angebundenen Terminverwaltungs- oder Praxisverwaltungssystemen des jeweiligen CGM-Unternehmens. Dabei werden die zur Identifikation und Zuordnung von Patienten zu bestehenden Datensätzen erforderlichen personenbezogenen Daten (insbesondere Patientenstammdaten) verarbeitet. Die Verarbeitung erfolgt ausschließlich in Echtzeit und dient der Vermeidung von Fehlzuordnungen sowie der korrekten Zuordnung von Terminbuchungen und sonstigen Vorgängen zu bestehenden Patientenprofilen. Eine darüberhinausgehende dauerhafte Speicherung dieser Daten durch den Auftragnehmer findet nicht statt; die Verarbeitung beschränkt sich auf eine kurzfristige, flüchtige Nutzung im Rahmen der jeweiligen Anfrage.

b. KI-Online Rezeption:

Die KI-Online Rezeption ist eine KI-gestützte Software-Anwendung, die eingehende patientenbezogene Anfragen über ein auf der Praxis-Website eingebettetes Widget in Echtzeit verarbeitet. Dabei werden die wesentlichen Informationen der Anfragen extrahiert und strukturiert zusammengefasst, sodass das Praxisteam das Anliegen effizient erfassen und weiterbearbeiten kann. Die Software nutzt

diese strukturierten Informationen zudem, um mittels eines Large Language Models unter Berücksichtigung von Wahrscheinlichkeitsaussagen passende Antworten zu generieren und eine natürliche Echtzeitkommunikation mit der anfragenden Person zu ermöglichen. Ziel ist es, digitale Anfragen – etwa Terminwünsche oder Rezeptanfragen – strukturiert an das Praxisteam weiterzuleiten und zu organisieren.

c. KI-Telefonassistent und KI-Online Rezeption:

Die Software integriert die beiden unter a) und b) beschriebenen Verarbeitungsweisen nach Umfang, Art und Zwecken und nutzt hierfür die unter 4. a) und b) beschriebenen Datenkategorien.

d. Support und Fernwartung

Im Rahmen von Supportleistungen, Fernwartung sowie zur Analyse, Qualitätssicherung und Verbesserung der Nutzung der Software kann der Auftragnehmer entsprechend den in den Ziffern 8.6 und 8.7 gewährten Befugnissen technische Analysewerkzeuge zur Auswertung von Nutzerinteraktionen einsetzen. Dabei werden Nutzungs- und Kommunikationsdaten, insbesondere Kommunikationsmetadaten, verarbeitet. Die Verarbeitung erfolgt ausschließlich zu Zwecken der Systemüberwachung, Fehleranalyse, Qualitätssicherung und Optimierung der Funktionsfähigkeit der Software sowie zur Unterstützung des Auftraggebers im Rahmen von Supportleistungen und zur Verbesserung der Nutzungsmöglichkeiten der Software im Interesse des Auftraggebers. Soweit hierfür personenbezogene Daten erforderlich sind, erfolgt eine personenbezogene Auswertung nur, soweit dies für den jeweiligen Support- oder Fernwartungsfall notwendig ist; eine darüberhinausgehende Nutzung zu Zwecken der allgemeinen Qualitätsverbesserung oder Weiterentwicklung der Software erfolgt ausschließlich auf Grundlage zuvor anonymisierter Daten.

3. Von der Datenverarbeitung Betroffene (Personenkategorien):

Für den KI-Telefonassistenten und/oder die KI-Online Rezeption werden Daten der folgenden Betroffenen verarbeitet:

- Auftraggeber
- Mitarbeiter des Auftraggebers
- Patienten und/oder (potenzielle) Kunden des Auftraggebers

4. Art der personenbezogenen Daten:

a) Datenkategorien des KI-Telefonassistenten (einschließlich Support)

- Personenstammdaten (z.B. Name und Adressdaten)
- Kommunikationsdaten (z. B. private Telefonnummer)
- Gesprächsinhalte
- Gesundheitsdaten (z.B. krankheitsbedingter Anlass der Terminanfrage; Gesundheitszustand)
- Nutzungsdaten (z.B. Benutzerkennungen, Kommunikationsmetadaten)

b) Datenkategorien der KI-Online Rezeption (einschließlich Support)

- Personenstammdaten (z.B. Name und Adressdaten)
- Kommunikationsdaten (z. B. private Emailadresse, Mobilfunknummer)
- Anfrageinhalte
- Gesundheitsdaten (z.B. krankheitsbedingter Anlass der Terminanfrage; Gesundheitszustand)
- Nutzungsdaten (z.B. Benutzerkennungen, Kommunikationsmetadaten)

c) Datenkategorien bei KI-Telefonassistent und KI-Online Rezeption
Die Software integriert die beiden unter a) und b) beschriebenen Verarbeitungsweisen nach Umfang, Art und Zwecken.

d) Zusätzliche Kategorien bei Nutzung angebundener Terminbuchungssystemen

- Versicherungsdaten (z. B. Versicherungstyp, Versicherungsnummer)
- Temporäre Identifikations- und Matchingdaten zur Zuordnung von Patientenprofilen

Die Auftragsverarbeitung umfasst die Verarbeitung besonders sensibler Daten, die nach Art. 9 DSGVO oder eine nationalen Vorschrift besonders zu schützen sind (konkret in Form von Gesundheitsdaten, sofern Anrufende diese, etwa durch Angaben zu ihrem Gesundheitszustand, machen); der Auftragnehmer hat hiervon Kenntnis.

5. Subunternehmer

Unternehmen	Anschrift/Land	Leistung	Datenbelegenheit; Angabe zu möglichem Drittstaatentransfer	Bei Drittstaatentransfer Angabe zu Absicherung nach Art. 44 ff. DSGVO
ElevenLabs Inc.	169 Madison Ave #2484 New York, NY 10016, United States	Text-zu-Sprache (TTS) und Sprache-zu-Text (STT) zur Echtzeit-Audioausgabe und Transkription im Rahmen der Nutzung des KI-Telefonassistenten (einschließlich Nutzung synthetischer Stimmprofile, optional praxisindividuelles „Voice-Cloning“ auf Basis vom Auftraggeber bereitgestellter Sprachaufnahmen; ausschließlich zur Leistungserbringung).	Verarbeitung erfolgt ausschließlich auf EU-Servern („Enfored EU Residency“) und ohne Speicherung von Inhaltsdaten („Zero Retention“); Kundeninhalte werden nicht gespeichert, nicht protokolliert und nicht zu Trainings/Auswertungszwecken genutzt. Ein Zugriff auf Kundeninhalte aus Staaten außerhalb der EU (einschließlich Fernzugriff) ist vertraglich ausgeschlossen.	N/A – ElevenLabs ist verpflichtet, ausschließlich Rechenzentren in der Europäischen Union zu nutzen und jegliche (Zwischen-) Speicherung von Inhaltsdaten der Gespräche zu unterlassen. Mangels Speicherung (Zero Retention) sind Zugriffsmöglichkeiten, etwa zu Supportzwecken, technisch ausgeschlossen. Die Verarbeitung der Daten einschließlich Kommunikation mit EU-Servern von ElevenLabs erfolgt zudem verschlüsselt.

CompuGroup Medical SE & Co. KGaA	Maria Trost 21 56070 Koblenz	<u>Support und Fernwartung:</u> Fernwartung, bzw. Remote Zugriff auf das System des Auftraggebers. <u>Systembereit-stellung:</u> (Hosting) und Support von: Software zur Fernwartung (AnyDesk) <u>Produktbetrieb:</u> Bereitstellung von Rechenkapazitäten auf EU-basierten Microsoft Azure-Servern (Cloud) zur DSGVO-konformen Verarbeitung. Sprache zu Text (STT), Text zu Sprache (TTS) und Nutzung synthetischer Stimmprofile im Rahmen des KI Telefonassistenten: Umwandlung eingehender Audiodaten aus Telefongesprächen in Text in Echtzeit („Transkription“) sowie Umwandlung generierter Antworttexte in Audiodaten zur Echtzeit Audioausgabe im Telefonkanal; Auswahl und Nutzung eines definierten synthetischen Stimmprofils ausschließlich zur Leistungserbringung. KI-Komponenten zur Erstellung strukturierter Zusammenfassungen aus Transkripten und zur Generierung von Antworttexten innerhalb des Produktflusses.	<u>Support und Fernwartung</u> Datenhosting erfolgt aus schließlich auf EU-Servern <u>Systembereit stellung:</u> Datenhosting erfolgt aus schließlich auf EU-Servern <u>Produktbetrieb:</u> Datenhosting erfolgt ausschließlich auf EU-Servern; auch Remote Support erfolgt innerhalb der EU (sog. Microsoft „EU Datengrenze“); in Ausnahmefällen sind Verarbeitungen aus den USA heraus möglich (z.B. in Notfällen wie globalen Sicherheitsvorfällen)	<u>Produktbetrieb:</u> Absicherung etwaiger Datentransfers durch das EU-US Datenschutzrahmenabkommen; ferner Absicherung durch EU-Standardvertragsklauseln und die Microsoft Transfer-Folgenabschätzung; Absicherung durch ein erweitertes Maßnahmekonzept (u.a. Verschlüsselung mit alleiniger Schlüsselverwaltung durch Auftragnehmer selbst; selektive Zugriffssteuerung mittels „Kunden-Lockbox“ durch Auftragnehmer)

		Einsatz von Sicherheits-maß nahmen wie Web Application Firewall (WAF).		

Twilio Germany GmbH	Rosenheimer Str. 143c, 81671 München	Bereitstellung von elektronischen Kommunikationsdiensten, einschließlich Zuweisung und Verwaltung von Telefonnummern, Durchleitung von Telefongesprächen und Kurznachrichten sowie Vorbereitung von Gesprächen für eine Transkription. Datenverarbeitung im Kontext von Telekommunikationsvorschriften und -standards.	Datenbelegenheit erfolgt in der EU und den USA; weitere Verarbeitung in Drittstaaten wie Indien (durch Twilio Inc. und andere Empfänger innerhalb der Twilio Gruppe) sind möglich entsprechend der Vorgaben der verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“) der Twilio Gruppe.	EU-US Datenschutzrahmenabkommen (Twilio Inc. u.a.); verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“) innerhalb der Twilio Gruppe; weitere Maßnahmen zur Reduzierung der Folgen der Datenübermittlung wie Richtlinien zum Umgang mit Herausgabeverlangen von Behörden, sofortige Löschung von Kommunkationsinhalten sowie Datenminimierung durch Anonymisierung oder Pseudonymisierung unter Ausschluss jedweder Re-Identifizierbarkeit durch Twilio bzw. die Twilio Gruppe.
Full-Story, Inc.	818 Mission Street, San Francisco, CA 94103, USA	Analyse von Nutzerinteraktionen innerhalb der Software zur Unterstützung von Support, Fehleranalyse, Produktverbesserung sowie statistischen Auswertungen der Nutzung. Verarbeitung von Nutzungsdaten, Interaktionsdaten und Kommunikationsmetadaten.	Die Verarbeitung der Daten erfolgt ausschließlich auf Servern innerhalb der Europäischen Union. Eine Übermittlung personenbezogener Daten in Drittländer findet nicht statt. Der Zugriff auf die Daten ist auf einen definierten und berechtigten Personenkreis beschränkt und erfolgt ausschließlich zu den vertraglich festgelegten Zwecken.	Der Auftragnehmer stellt durch entsprechende vertragliche und technische Maßnahmen sicher, dass sämtliche Daten ausschließlich innerhalb der EU verarbeitet werden und kein Zugriff aus Drittländern erfolgt.

Anlage 2a – Technisch-organisatorische standortbezogene Maßnahmen der CGM

Technische und organisatorische Maßnahmen zum Datenschutz und Datensicherheit

Die technischen und organisatorischen Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus für die Datenverarbeitung am jeweiligen Standort des Auftragnehmers, (die **standortbezogenen Maßnahmen**) umfassen die folgenden Maßnahmekategorien entsprechend den Zielkategorien des Art. 32 Abs. 1 DSGVO.

1. **Vertraulichkeit (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**
    - Trennungskontrolle (Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)
    - Anonymisierung/Pseudonymisierung (Maßnahmen zur Datenminimierung, soweit in der AVV vorgesehen)
    - Zugangskontrolle (Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können)
    - Zugriffskontrolle (Maßnahmen, die gewährleisten, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können)
    - Zutrittskontrolle/Physische Sicherheit (Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren)
2. **Integrität (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**
    - Eingabekontrolle (Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)
3. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DS-GVO)**
    - Verfügbarkeitskontrolle (Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind)
    - Rasche Wiederherstellbarkeit (Maßnahmen, die eine rasche Wiederherstellung von personenbezogenen Daten gewährleisten Art. 32 Abs. 1 lit. c DS-GVO)
4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**
    - Prüf- und Kontrollmechanismen des Zentralen Datenschutzmanagementsystems der sowie den zentralen Informationssicherheitsmanagementsystems der CompuGroup Medical SE & Co. KGaA (zertifiziert nach ISO 27001:2022)
    - Auftragskontrolle (Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und gemäß dieser AVV verarbeitet werden)
    - Weitergabekontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt verarbeitet werden können, und dass festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten erfolgt)
    - Datenschutzfreundliche Voreinstellungen („Privacy by default“ Maßnahmen des Produkts zur Minimierung der Datenverarbeitung und Steuerung durch den Anwender)
    - Datenschutz durch Technikgestaltung im Produktlebenszyklus („Privacy by Design“ Prozesse, die darauf abzielen, eine Datenschutzkonformität während des gesamten Produktlebenszyklus sicherzustellen)

Die technischen und organisatorischen Maßnahmen für den Standort Koblenz und das Rechenzentrum in Frankfurt sind dem Dokument „CGM TOM Koblenz und Frankfurt V15_DE.pdf“ zu entnehmen. Dieses können Sie bei dem in **Anlage 3** genannten Datenschutzkontakt anfragen. Diese Maßnahmen finden insbesondere im Kontext der Fernwartung/Produktsupports Anwendung.

Anlage 2b – Technisch-organisatorische produktbezogene Maßnahmen

Technische und organisatorische Maßnahmen zum Datenschutz und Datensicherheit

Die technischen und organisatorischen Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus für die Datenverarbeitung der Software (KI-Telefonassistent und/oder KI-Online Rezeption), einschließlich der Applikation und der (Cloud-)Infrastruktur (die **produktbezogenen Maßnahmen**) umfassen die folgenden Maßnahmekategorien entsprechend den Zielkategorien des At. 32 DSGVO.

1. **Vertraulichkeit (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**
    - Trennungskontrolle (Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)
    - Anonymisierung/Pseudonymisierung (Maßnahmen zur Datenminimierung, soweit in der AVV vorgesehen einschließlich Maßnahmen des Unterauftragnehmers für elektronische Kommunikation)
    - Zugangskontrolle (Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können)
    - Zugriffskontrolle (Maßnahmen, die gewährleisten, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können)
2. **Datenverschlüsselung (bei Speicherung und Transfer gemäß den gesetzlichen und regulatorischen Anforderungen) Integrität (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**
    - Eingabekontrolle (Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)
3. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DS-GVO)**
    - Verfügbarkeitskontrolle (Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind)
    - Rasche Wiederherstellbarkeit (Maßnahmen, die eine rasche Wiederherstellung von personenbezogenen Daten gewährleisten Art. 32 Abs. 1 lit. c DS-GVO)
4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**
    - Prüf- und Kontrollmechanismen des Zentralen Datenschutzmanagementsystems der CompuGroup Medical SE & Co. KGaA
    - Auftragskontrolle (Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und gemäß dieser AVV verarbeitet werden)
    - Weitergabekontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt verarbeitet werden können, und dass festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten erfolgt)
    - Datenschutzfreundliche Voreinstellungen („Privacy by default“ Maßnahmen des Produkts zur Minimierung der Datenverarbeitung und Steuerung durch den Anwender)
    - Datenschutz durch Technikgestaltung im Produktlebenszyklus („Privacy by Design“ Prozesse, die darauf abzielen, eine Datenschutzkonformität während des gesamten Produktlebenszyklus sicherzustellen)

Die einzelnen produktbezogenen Maßnahmen sind getrennt dokumentiert (und ergänzen die standortbezogenen Maßnahmen der Anlage 2a). Diese Dokumentation können Sie bei dem in **Anlage 3** genannten Datenschutzkontakt anfragen. Diese Maßnahmen finden insbesondere im Kontext des Hostings und Betriebs des Produkts Anwendung.

Der beauftragte Subunternehmer Microsoft ist sowohl nach dem ISO 27001:2022 Standard- als auch nach dem BSI-Standard C5-zertifiziert. In diesem Zusammenhang trifft Microsoft auch technisch-organisatorische Maßnahmen zur Sicherstellung einer gemäß dem Stand-der-Technik angemessen geschützten Cloud-Infrastruktur. Weitergehende Informationen finden sich auf der Website des Subunternehmers Microsoft unter Dokumentation zur Azure-Compliance | Microsoft Learn.

Der beauftragte Subunternehmer Twilio ist sowohl nach ISO 27001 als auch ISO 27017 und 27018 zertifiziert. Weitere Dokumentation zur Sicherheit, Compliance und Datenschutz bei Twilio Diensten ist verfügbar unter Twilio Security | Twilio.

Anlage 3 – Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers

Der Datenschutzbeauftragte des Auftragnehmers ist wie folgt zu erreichen:

Abteilung “Group Data Privacy & Security”
CompuGroup Medical SE & Co. KGaA
Maria Trost 21
56070 Koblenz

E-Mail: DPO@cgm.com

Version vom 27.04.2026