

# Auftragsverarbeitungsvertrag

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

Die CompuGroup Medical Deutschland AG, Maria Trost 2, D-56070 Koblenz (der **Auftragnehmer oder CGM**) ist einer der führenden IT-Dienstleister im Gesundheitssektor. Der Auftragnehmer verarbeitet personenbezogene Daten für den Kunden (der **Auftraggeber**) im Rahmen eines oder mehrerer Hauptverträge (Auftragnehmer und Auftraggeber zusammen die **Parteien** oder jeweils einzelne eine **Partei**). Der Auftraggeber ist hierbei Verantwortlicher gem. Art. 4 Nr. 7 DSGVO, der Auftragnehmer Auftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO.

Sofern die im Vertrag zu CGM one CheckIn (der **Hauptvertrag**) vereinbarten Leistungen die Verarbeitung personenbezogener Daten gemäß der beigefügten **Anlage 1** betreffen, verarbeitet der Auftragnehmer diese personenbezogenen Daten im Auftrag gem. Art. 28 Datenschutzgrundverordnung (**DSGVO**). Hierzu schließen die Vertragsparteien den nachfolgenden Auftragsverarbeitungsvertrag (der **Vertrag** oder **AVV**).

Die Regelungen dieses Vertrags und zugleich abgeschlossener allgemeiner Geschäftsbedingungen ergänzen sich und bestehen nebeneinander. Bei etwaigen Widersprüchen geht dieser Vertrag den allgemeinen Geschäftsbedingungen vor.

### § 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 im **Anlagenkonvolut 1** als Gegenstand der Auftragsverarbeitung gelistet sind. Für jeden gesonderten Gegenstand der Auftragsverarbeitung zwischen den Parteien ist eine eigene **Anlage 1** zu führen. Die **Anlagen 1** werden 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 1.1** zum jeweiligen Gegenstand gem. § 1.1 gelistet.
- 1.3 Die Verarbeitung personenbezogener Daten unter diesem Vertrag erfolgt in einem Mitgliedsstaat 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.

## § 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. Haben die Parteien nach den Hauptverträgen, deren Leistungen Gegenstand dieses Auftragsverarbeitungsvertrages sind, eine befristete Leistungserbringung und / oder ein Auflösungsdatum vereinbart, so endet dieser Auftragsverarbeitungsvertrag auch mit dem Ablauf dieses Datums, ohne dass es einer Kündigung bedarf. Der Auftragnehmer hat die Verarbeitung personenbezogener Daten in diesem Falle mit dem Ablaufdatum einzustellen. Dasselbe gilt mit dem Beendigungsdatum des jeweiligen Hauptvertrages, wenn dieser 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 Auftragnehmer 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 2 a und Anlage 2 b beigelegt.

- 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 unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, zu den in Anlage 2 a; Anlage 2 b 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 Betroffenrechte 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 vom Auftragnehmer auch gegenüber dem 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 stehen, 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 im Einklang mit Unionsrecht oder dem Recht eines Mitgliedstaats stehenden gesetzlichen Pflichten, denen 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 führt Verarbeitungen gemäß § 8.6 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.

## **§ 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 gegenüber etwaigen Haftungsbegrenzungen im Hauptvertrag oder allgemeinen Geschäftsbedingungen der Parteien.

## **§ 10 Schlussbestimmungen**

- 10.1 Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform (einschließlich E-Mail, DocuSign oder Bestätigung der Änderung über ein elektronisches Formular). Dies gilt auch für den Verzicht auf dieses Formerfordernis. Sofern Änderungen und Ergänzungen zur Einhaltung der datenschutzrechtlichen Anforderungen erforderlich sind, etwa aufgrund externer Entwicklungen notwendiger Anpassungen der Datensicherheitsanforderungen, oder aus triftigen Gründen wie Änderungen des Hauptvertrages, Anpassungen zugunsten der Auftraggeber oder Weiterentwicklungen ohne nachteilige Auswirkungen für die Auftraggeber erfolgen, werden diese in geeigneter Weise bekannt gegeben und gelten als durch den Kunden bestätigt, wenn diesen nicht innerhalb der vom Auftragnehmer gesetzten Frist entsprechend § 6.2 dieses Vertrages widersprochen wird. Der Kunde nimmt diese Änderungen durch fortgesetzten Bezug der Leistungen aus dem Hauptvertrag an.
- 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 von:  
CGM one CheckIn

### **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:

- Hosting und Betrieb der Anwendung CGM one Checkin auf mobilen Endgeräten
- Bereitstellung der Schnittstelle CGM myTI zur Anbindung an die Fachdienste der Telematikinfrastruktur
- Kundensupport in Form von Fernwartung und Arbeiten vor Ort

### **3. Von der Datenverarbeitung Betroffene (Personenkategorien):**

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

### **4. Art der personenbezogenen Daten:**

- Personenstammdaten
- Patientenstammdaten
- Berufliche und private Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsabrechnungs- und Zahlungsdaten von Kunden und Lieferanten
- Gesundheitsdaten
- Sozialdaten
- Nutzungsdaten (z.B. Benutzerkennungen von Arbeitsplätzen und/oder Netzwerkgeräten)

**Die Auftragsverarbeitung umfasst die Verarbeitung besonders sensibler Daten, die nach Art. 9 DSGVO oder einer nationalen Vorschrift besonders zu schützen sind; der Auftragnehmer hat hiervon Kenntnis.**

## 5. Subunternehmer

Unternehmen	Anschrift/Land	Leistung	Datenbelegbarkeit; Angabe zu möglichem Drittstaatentransfer	Bei Drittstaatentransfer Angabe zu Absicherung nach Art. 44 ff. DSGVO
CGM Systemhaus GmbH	Maria Trost 21 56070 Koblenz	Durchführung von Produktinstallationen, Schulungen und Kundensupport mittels Fernwartung.	Datenverarbeitung erfolgt ausschließlich auf EU-Servern.	n/a
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Server Hosting für online Ausfüllen von Inhalten	Datenverarbeitung erfolgt ausschließlich auf EU-Servern.	n/a
Strato AG	Otto-Ostrowski-Straße 7 10249 Berlin	DNS-Dienste	Datenverarbeitung erfolgt ausschließlich auf EU-Servern.	n/a
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>Systembereitstellung:</u> Hosting und Support von: Software zur Fernwartung (AnyDesk)	Datenverarbeitung erfolgt ausschließlich auf EU-Servern.	n/a

## **Anlage 2 – Technisch-organisatorischen Maßnahmen bei CGM**

### **Anlage 2 a: Allgemeine technisch-organisatorische Maßnahmen:**

Die technischen und organisatorischen Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus für die Datenverarbeitung am jeweiligen Standort des Auftragnehmers, (die **standort-bezogenen Maßnahmen**) umfassen die folgenden Maßnahmenkategorien 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 DSGVO; 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“ 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 des Produkts bzw. Dienstes, einschließlich der Applikation und der Infrastruktur (die **produktbezogenen Maßnahmen**) umfassen die folgenden Maßnahmekategorien entsprechend den Zielkategorien des Art. 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)
- 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. 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.

#### **Anlage 3 – Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers**

Datenschutzbeauftragter bei CompuGroup Medical Deutschland AG ist Hans Josef Gerlitz, CompuGroup Medical Deutschland AG, Maria Trost 21, 56070 Koblenz.

E-Mail: HansJosef.Gerlitz@cgm.com