Datenschutzerklärung der

CompuGroup Medical Deutschland AG – Business Area Connectivity

1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Der Produktbereich der CompuGroup Medical Deutschland AG erachtet den verantwortungsvollen Umgang und die Achtung des Schutzes personenbezogener Daten als obersten Grundsatz. Die CompuGroup Medical Deutschland AG misst der Einhaltung aller relevanten Gesetze bei der Speicherung und Verarbeitung der personenbezogenen Daten stets höchste Priorität zu.

Der Mutterkonzern, die CompuGroup Medical SE & Co. KGaA (CGM), hat ein zentrales Datenschutzmanagement eingeführt, das innerhalb aller CGM-Unternehmen ein einheitliches und hohes Niveau für den Schutz personenbezogener Daten gewährleistet und die Einhaltung der entsprechenden Datenschutzgesetze sicherstellt.

Mit dieser Datenschutzerklärung stellen wir Ihnen Informationen über den Umgang mit Daten innerhalb der CGM im Zusammenhang mit dem Einsatz unserer Produkte zur Verfügung, so dass auch Sie Ihre Patienten und Kunden entsprechend informieren können. Diese Datenschutzerklärung bezieht sich auf CGM MANAGED TI.

Diese Datenschutzerklärung stellen wir als datenschutzrechtliche Verantwortlicher zur Verfügung.

Die aktuellste Version dieser Datenschutzerklärung finden Sie immer unter cgm.com/protect-download

2. Zweck von CGM MANAGED TI

Die CGM MANAGED TI Lösung mit dem CGM TI-GATEWAY stellt eine zentrale Komponente der Telematikinfrastruktur (TI) dar und bildet die Schnittstelle zwischen der zentralen TI-Infrastruktur und der dezentralen Umgebung. Es ermöglicht die sichere und gesicherte Verbindung zum VPN-Zugangsdienst der TI, indem es Zugriffsdienste und Teilfunktionen des Konnektors in einer integrierten Lösung vereint.

3. Verarbeitung von personenbezogenen Daten durch CGM

CompuGroup Medical Deutschland AG, Business Area Connectivity speichert bei der Verwendung der angebotenen Produkte oder Dienste folgende Arten von Daten auf ihren Servern:

- **Vertrags- und Registrierungsdaten**
- **Daten zum technischen Betrieb**

Die Daten wie sämtliche Vertragsdaten, sämtliche Registrierungsdaten und sämtliche Daten zum technischen Betrieb werden nur so lange verarbeitet, wie das datenschutzrechtlich zulässig ist. Regelmäßig werden wir diese, spätestens nach Beendigung des Vertrages mit Ihnen und Ablauf der gesetzlichen Aufbewahrungsrechte und -pflichten, insbesondere aus dem Handels- und Steuerrecht, löschen.

3.1 Vertrags- und Registrierungsdaten

Vertrags- und Registrierungsdaten dienen der Zuordnung und Betreuung eines zwischen der Praxis und CompuGroup Medical Deutschland AG, Business Area Connectivity geschlossenen Vertragsverhältnisses. Zu diesen Daten gehören:

- Institutionsdaten
  - Institutionsname
  - Institutionstyp
  - Adresse
  - Telefonnummer
  - BSNR (sofern vorhanden)
  - NBSNR (sofern vorhanden)
- Arztdaten
  - Anrede / Titel
  - Vorname / Nachname
  - Namenszusatz
  - LANR (sofern vorhanden)
  - Fachrichtung
  - E-Mail-Adresse

Des Weiteren optional hinzugefügt werden können:

- Geschlecht
- Geburtsdatum
- Land
- Telefon (privat)
- Telefon (mobil)
- Faxnummer
- Bankdaten (Einzugsermächtigung)
- Namen von Ansprechpartnern

Im Rahmen der Vertrags- und Geschäftsbeziehung bekannt gewordene personenbezogene Daten werden von CompuGroup Medical Deutschland AG, Business Area Connectivity gespeichert und verarbeitet, soweit dies zur Durchführung des Vertrages, insbesondere zur Auftragsabwicklung und Kundenbetreuung, notwendig ist (Art. 6 I 1 b DSGVO).

Darüber hinaus können wir diese Daten aus unserem berechtigten Interesse heraus verarbeiten, um die Geschäftsbeziehung mit Ihnen aufrecht zu erhalten, zu pflegen oder Sie über neue Produkte bzw. neue Entwicklungen zu informieren (Art. 6 I 1 f DSGVO). Ebenso können wir aus berechtigten Interessen diese Daten innerhalb des CGM-Konzerns an Gruppenunternehmen übermitteln, um unsere Produktqualität und die Marktrelevanz zu messen und zu verbessern, um auch zu Ihren Gunsten die besten Produkte anbieten und diese mit werblichen Maßnahmen fördern zu können (Art. 6 I 1f DSGVO). Dem können Sie jederzeit für die Zukunft widersprechen, wie unter „Rechte der Betroffenen“ näher erläutert.

CompuGroup Medical Deutschland AG, Business Area Connectivity arbeitet mit der CGM SE & Co. KGaA arbeitsteilig in gemeinsamer Verantwortlichkeit für die Bereitstellung von IT für die Kundenkommunikation, das Kundencontrolling, Finance, Marketing und Customer World zusammen. Hierbei werden u.U. auch personenbezogene Kundendaten verarbeitet, beispielsweise der Name eines Praxisinhabers, nicht hingegen die von Ihnen in unseren Produkten abgespeicherte Daten Ihrer Patienten. Die CGM SE & Co.KAaA stellt in diesen Bereichen die Tools bereit. Wir melden unsere Bedarfe an und nutzen die Tools. Über diese Datenverarbeitung in Gemeinsamer Verantwortlichkeit haben wir mit der CGM SE & CO. KGaA einen Vertrag mit folgendem wesentlichen Inhalt gem. Art. 26 Abs. 2 DSGVO geschlossen: Informationen nach Art. 13, 14 DSGVO werden von jeder Partei selbst bereitgestellt, dieser Pflicht kommen wir mit der vorliegenden Übersicht nach. Betroffene können sich zur Geltendmachung ihrer Rechte an jeden der Gemeinsam Verantwortlichen wenden. Jede Partei ist in ihrem jeweiligen Wirk- und Zuständigkeitsbereich selbst für die Erfüllung von Betroffenenrechten nach Art. 15-22 DSGVO und für die Einhaltung der gesetzlichen Bestimmungen, insbesondere die Rechtmäßigkeit der durch sie im Rahmen der Gemeinsamen Verarbeitung durchgeführten Datenverarbeitungen zuständig.

Die Vertragsdaten werden zudem auf dem CGM Server in Deutschland gespeichert. Wir setzen dafür die CGM SE & Co. KGaA als Rechenzentrums Betreiberin und Auftragsverarbeiterin datenschutzkonform ein.

Ferner werden wir die Sie betreffenden Daten mit Ihrer (freiwilligen) Einwilligung auch zu anderen Zwecken verarbeiten, insbesondere für produkt-

bezogene Umfragen und Marketingzwecke entsprechend den weitergehenden Ausführungen in der jeweiligen Einwilligung (Art. 6 I 1 a DSGVO). Eine uns gegebene Einwilligung können Sie jederzeit für die Zukunft widerrufen, wie unter „Rechte der Betroffenen" näher erläutert.

Die Weitergabe, der Verkauf oder sonstige Übermittlung personenbezogener Daten an außenstehende Dritte erfolgt nicht, es sei denn, dass dies zum Zwecke der Vertragsabwicklung erforderlich ist oder eine ausdrückliche Einwilligung vorliegt. Es kann beispielsweise erforderlich sein, dass der Produktbereich CompuGroup Medical Deutschland AG, Business Area Connectivity Anschrift und Bestelldaten bei Produktbestellung an Vertriebs- und Servicepartner sowie die Anschrift an externe Produktionsfirmen zur Erstellung und dem Versand der Update-Datenträger weitergibt.

3.2 Daten zum technischen Betrieb

CGM erhebt Daten zum technischen Betrieb, um die in einem Vertrag zugesicherten Leistungen bereitstellen zu können und vorgeschriebene Spezifikationen der gematik GmbH (gematik), zu erfüllen. Folgende Daten zum technischen Betrieb werden erhoben:

1. **Nutzerdaten**
   Die Nutzung von CGM MANAGED TI auf Basis des CGM TI-Gateways erfordert ein Nutzerkonto. In diesem Zusammenhang werden folgende Daten zum technischen Betrieb gespeichert:
   - technische ID (dient der Identifikation und Zuordnung von Ressourcen zum Nutzerkonto)
   - Hash des Passworts (dient der Verifikation des Passworts beim Login)
   - TOTP-Secret (dient der Erzeugung und Prüfung eines zeitbasierten Einmalpassworts)
   - Fehlgeschlagene Login-Versuche (dient der temporären Sperrung ab einem bestimmten Schwellwert)
   - Letzter Login
2. **Nutzern indirekt zugeordnete Daten**
   Nutzer sind Organisationen zugeordnet. Für die jeweiligen Organisationen werden z. B. Informationen über VPN-Profile von Leistungserbringer-Institutionen, oder die Zuordnung von Dienstleistern vor Ort (DVO) gespeichert.
3. **Betriebsdaten**
   Gemäß Spezifikationen der gematik sind Betriebsdaten zu erfassen und zu melden. Dazu gehören beispielsweise Metriken, in denen Summen verschiedener Ereignisse gesammelt werden, aber auch Rohdaten (z. B. Auf- und Abbau von VPN-Tunneln) welche keine Rückschlüsse auf Benutzer zulassen.
4. **Logging**
   Die Anwendungen des Zugangsmoduls (Bestandteil des CGM TI-Gateway) speichern Logdaten wie z. B. IP-Adressen des Nutzers und Login-Name (E-Mail-Adresse) zur Gewährleistung eines sicheren und auditierbaren Betriebs (Art. 32 DSGVO).

Im Übrigen verarbeiten wir technische Daten nur im Fall Ihrer gesonderten Einwilligung (Art. 6 I 1 a DSGVO)) oder einer spezifischen gesetzlichen Erlaubnis. Regelmäßig erbringt CGM diese Angebote als Auftragsverarbeiter auf Grundlage eines Auftragsverarbeitungsvertrages nach Art. 28 DSGVO.

Im Rahmen der Fernwartung wird die CGM nur nach gesonderter Vereinbarung auf die Systeme des Auftraggebers zugreifen; welche Datenarten dabei verarbeitet werden und alle weiteren relevanten Informationen zum Datenschutz ergeben sich aus der zugrundeliegenden Auftragsverarbeitungsvereinbarung.

Die Daten zum technischen Betrieb werden auf dem Server der CGM in Deutschland gespeichert.

4. Datenübermittlung

CGM MANAGED TI übermittelt Daten elektronisch auf gesetzlicher, vertraglicher oder einwilligungsbasierter Grundlage nur nach Interaktion durch den Anwender oder – entsprechend der Zustimmung- automatisiert.

Die Einhaltung der verpflichtenden Anforderungen der gematik ist in CGM MANAGED TI gewährleistet.

Eine Übermittlung in Drittstaaten außerhalb des europäischen Wirtschaftsraums (EWR) findet nicht statt, sofern sich diese nicht aus anderen, im Rahmen der Leistungserbringung eingesetzten Produkten oder den Umständen des Zugriffs (etwa Zugriff durch den Nutzer auf das webbasierte Nutzerportal von außerhalb des EWR) ergibt.

5. Verpflichtung auf Vertraulichkeit, Datenschutzschulungen

Patientendaten, insbesondere die Gesundheitsdaten, unterliegen neben den Sicherheitsanforderungen der allgemeinen Datenschutzgesetze (DSGVO und BDSG) zusätzlich strengen Auflagen aus dem Strafgesetzbuch (StGB) sowie den Sozialgesetzbüchern (SGB) und werden, sofern sie uns überhaupt bekannt werden, von CGM besonders sensibel behandelt.

Wir greifen auf diese nur im vereinbarten Rahmen zu und beschränken den Zugriff auf Vertragsdaten, Protokolldaten und Daten zum technischen Betrieb auf Mitarbeiter und Auftragnehmer der CGM, für die diese Informationen zwingend erforderlich sind, um die Leistungen aus unserem Vertrag zu erbringen. Diese Personen sind an die Einhaltung dieser Datenschutzerklärung und an Vertraulichkeitsverpflichtungen (DSGVO, §203 StGB) verpflichtend gebunden. Die Verletzung dieser Vertraulichkeitsverpflichtungen kann mit Kündigung und Strafverfolgung geahndet werden.

Die Mitarbeiter werden regelmäßig auf Datenschutz geschult.

6. Sicherheitsmaßnahmen / Vermeidung von Risiken

Die CGM trifft alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen, um Ihre personenbezogenen Daten sowie Ihre Kundendaten (Patientendaten) vor unerlaubtem Zugriff, unerlaubten Änderungen, Offenlegung, Verlust, Vernichtung und sonstigen Missbrauch zu schützen. Hierzu gehören interne Prüfungen unserer Vorgehensweise bei der Datenerhebung, -speicherung und -verarbeitung, weiterhin Sicherheitsmaßnahmen zum Schutz vor unberechtigtem Zugriff auf Systeme, auf denen wir Vertragsdaten oder Daten zum technischen Betrieb speichern.

7. Technische und organisatorische Maßnahmen

Um die Datensicherheit zu gewährleisten, überprüft die CGM regelmäßig den Stand der Technik. Hierzu werden unter anderem typische Schadenszenarien ermittelt und anschließend der Schutzbedarf für einzelne personenbezogene Daten abgeleitet und in Schadenskategorien eingeteilt. Zudem wird eine Risikobewertung durchgeführt.
Weiterhin dienen differenzierte Penetrationstest zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen werden folgende Grundsätze normiert:

- **Backup / Datensicherung (Praxis)**
  Zur Vorbeugung der Datenverluste werden die Daten regelmäßig gesichert (Backup des AIS und der Zusatzprodukte).
- **Privacy by design**
  Die CGM achtet darauf, dass Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden. Somit wird dem Umstand vorgebeugt, dass die Vorgaben des Datenschutzes und der Datensicherheit erst nach dem Bereitstellen von IT-Systemen durch teure und zeitaufwendige Zusatzprogrammierungen umgesetzt werden müssen. Bereits bei der Herstellung werden Möglichkeiten wie Deaktivierung von Funktionalitäten, Authentifizierung oder Verschlüsselungen berücksichtigt.
- **Privacy by default**
  Weiterhin sind die Produkte der CGM im Auslieferungszustand bereits datenschutzfreundlich voreingestellt, so dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind.
- **Kommunikation per E-Mail (Praxis / CGM)**
  Sollten Sie mit der CGM per E-Mail in Kontakt treten wollen, weisen wir darauf hin, dass die Vertraulichkeit der übermittelten Informationen nicht gewährleistet ist. Der Inhalt von E-Mails kann von Dritten eingesehen werden. Wir empfehlen Ihnen daher, uns vertrauliche Informationen ausschließlich über den Postweg zukommen zu lassen.
- **Fernwartung**
  In Ausnahmefällen kann es vorkommen, dass Mitarbeiter oder Auftragnehmer der CGM auf Patienten- und Kundendaten und somit evtl. auch auf ihre Praxisdaten zurückgreifen müssen. Hierzu gibt es zentrale Regelungen der CGM; dies erfolgt stets nur dann, wenn ein Fernwartungsauftrag besteht und dazu ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen wurde.
    - Die Fernwartungs-Zugänge bleiben geschlossen und werden nur durch Kunden frei geschaltet.
    - Passwörter zu Kundensystemen werden nur für die Fernwartung erteilt.
    - Besondere Tätigkeiten werden durch das 4-Augenprinzip über qualifizierte Personen abgesichert
    - Wir verwenden Fernwartungsmedien, bei welchen der Kunde aktiv den Zugang freigeben muss und die Aktivitäten mitverfolgen kann.
    - Die Dokumentation des Fernwartungszugriffes erfolgt im CRM-System der CGM. Dokumentiert werden: Ausführender Mitarbeiter, Zeitpunkt (Datum/Uhrzeit), Dauer, Zielsystem, das Fernwartungsmedium, kurze Beschreibung der Tätigkeit. Bei kritischen Tätigkeiten werden auch die nach dem als 4-Augenprinzip herangezogenen Mitarbeiter erfasst.
    - Die Aufzeichnung der Sitzungen ist verboten

8. Rechte der Betroffenen

Personenbezogene Daten des Arztes und der Praxismitarbeiter

Sie haben das Recht auf Auskunft über zu Ihrer Person gespeicherten Daten sowie Rechte auf Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Sperrung oder Löschung dieser Daten.

Bei der CGM erteilten Einwilligungen haben Sie das Recht, diese jederzeit mit der Wirkung für die Zukunft zu widerrufen.

Darüber hinaus haben Sie das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Meinung sind, dass wir Ihre personenbezogenen Daten nicht richtig verarbeiten.

Personenbezogene Daten Ihrer Patienten

Ihre Patienten haben das Recht auf Auskunft über zu ihnen gespeicherten Daten sowie unter bestimmten Voraussetzungen auf Mitnahme dieser Daten (Recht auf Datenportabilität) sowie ggf. Rechte auf Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Sperrung oder Löschung dieser Daten. Bei den Löschanfragen sind Sie jedoch gesetzlich verpflichtet, die geltenden Aufbewahrungsfristen zu beachten.

Bei der Ihnen erteilten Einwilligungen haben Ihre Patienten das Recht, diese jederzeit mit der Wirkung für die Zukunft zu widerrufen.

Darüber hinaus haben sie das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Meinung sind, dass Sie Ihre personenbezogenen Daten nicht richtig verarbeiten.

9. Durchsetzung

Die CGM überprüft regelmäßig und durchgängig die Einhaltung dieser Datenschutzbestimmungen. Erhält die CGM formale Beschwerdeschriften, wird sie mit dem Verfasser bezüglich seiner Bedenken Kontakt aufnehmen, um eventuelle Beschwerden hinsichtlich der Verwendung von persönlichen Daten zu lösen. Die CGM verpflichtet sich, dazu kooperativ mit den entsprechenden Behörden, einschließlich Datenschutzaufsichtsbehörden, zusammenzuarbeiten.

10. Änderungen an dieser Datenschutzerklärung

Beachten Sie, dass diese Datenschutzerklärung von Zeit zu Zeit ergänzt und geändert werden kann. Sollten die Änderungen wesentlich sein, werden wir eine ausführlichere Benachrichtigung ausgeben. Jede Version dieser Datenschutzbestimmungen ist anhand ihres Datums- und Versionsstandes in der Fußzeile dieser Datenschutzerklärung (Stand) zu identifizieren. Außerdem archivieren wir alle früheren Versionen dieser Datenschutzbestimmungen zu Ihrer Einsicht auf Nachfrage beim Datenschutzbeauftragten der CGM SE & Co. KGaA.

11. Verantwortlich für den CompuGroup Medical Deutschland AG, Business Area Connectivity

CompuGroup Medical Deutschland AG

Maria Trost 21
56070 Koblenz

12. Datenschutzbeauftragter

Bei Fragen hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten können Sie sich an den Datenschutzbeauftragten wenden, der im Falle von Auskunftsersuchen oder Beschwerden Ihnen zur Verfügung steht

Abteilung „Group Data Privacy & Security“
CompuGroup Medical SE & Co. KGaA
Maria Trost 21
56070 Koblenz
E-Mail: DPO@cgm.com

13. Zuständige Aufsichtsbehörde

Für die CompuGroup Medical Deutschland AG, Business Area Connectivity ist

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34
55116 Mainz

als Aufsichtsbehörde zuständig.