Datenschutzerklärung der

CompuGroup Medical Deutschland AG – Division Connectivity

1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Die CGM erachtet den verantwortungsvollen Umgang und die Achtung des Schutzes personenbezogener Daten als obersten Grundsatz.

Die CGM sichert stets die genaue Einhaltung aller relevanten Gesetze bei der Speicherung und Verarbeitung der personenbezogenen Daten ab.

CGM SE & Co. KGaA 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 erfüllen wir unsere Informationspflichten und stellen Ihnen Informationen über den Umgang mit Daten bei der CGM zur Verfügung. Diese Datenschutzerklärung bezieht sich auf das Produkt CGM PROTECT EndPoint 360°.

Die aktuelle Version dieser Datenschutzerklärung wird Ihnen auf Anfrage gerne bei dem Kundendienst unter: service@telemed.de oder unter Tel. 0261/8000 2007 zur Verfügung gestellt.

2. CGM PROTECT EndPoint 360°

Die CGM PROTECT EndPoint 360° ist eine hochwertige technische Lösung zum Schutz Ihres Netzwerkes.
CGM PROTECT EndPoint 360° leistet fortgeschrittene Cybersicherheit zur Abwehr von Malware mit Präventions-, Erkennungs- und Wiederherstellungsfunktionen. Überwacht, erfasst und kategorisiert laufende IT-Prozesse auf allen Endpunkten in der Organisation des Auftraggebers.
Die CGM PROTECT EndPoint 360° verfügt über ein eigenes Benutzerrechte-Konzept. Der Zugriff auf die Software ist somit nur berechtigten Personen gestattet. Das Konzept regelt neben dem Zugriff auf das Produkt selbst auch die Zuteilung von Schreib- und Leserechten.

3. Verarbeitung von personenbezogenen Daten durch CGM

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Wir verpflichten uns gemäß Datenschutzgesetz, sämtliche Vertragsdaten, sämtliche Protokolldaten und sämtliche Daten zum technischen Betrieb nach Kündigung Ihres Vertrages zu löschen, sobald keine gesetzlichen Aufbewahrungsrechte und -pflichten mehr bestehen. Wir sind insbesondere gesetzlich verpflichtet, Handels- und Steuerrechtliche Aufbewahrungsfristen zu beachten, die über die Dauer des Vertragsverhältnisses hinausgehen können. Daten zum technischen Betrieb werden i.d.R. nur so lange vorgehalten, wie es technisch notwendig ist und spätestens nach Kündigung Ihres Vertrages gelöscht.

3.1 Vertrags- und Registrierungsdaten

Die für den Vertragsabschluss notwendige Daten sind:

- Vorname / Nachname des Praxisinhabers
- Bezeichnung der Einrichtung
- Postalische Anschrift
- Telefonnummer
- E-Mail-Adresse
- Bankdaten (Einzugsermächtigung)
- Name des zuständigen Vertriebs -und Servicepartners

Im Rahmen der Vertrags- und Geschäftsbeziehung bekannt gewordene personenbezogene Daten werden von CGM nur gespeichert und verarbeitet, soweit dies zur Durchführung des Vertrages, insbesondere zur Auftragsabwicklung und Kundenbetreuung, notwendig ist.

Die Weitergabe, der Verkauf oder sonstige Übermittlung personenbezogener Daten an Dritte erfolgt nicht, es sei denn, dass dies zum Zwecke der Vertragsabwicklung oder des Betriebes erforderlich ist oder eine ausdrückliche Einwilligung vorliegt. Es kann beispielsweise erforderlich sein, dass CGM Ihre Anschrift bei Produktbestellung an Vertriebs- und Servicepartner oder vertraglich gebundene Logistiker weitergibt.

Die Vertrags- und Registrierungsdaten werden auf den sicheren CGM Servern in Deutschland gespeichert.

3.2 Daten zum technischen Betrieb

Während der Nutzung des Produktes werden auch Daten zum technischen Betrieb verarbeitet. Sie werden benötigt, um die reibungslose Bereitstellung der im Vertrag zugesicherten Leistungen sicherzustellen. Die CGM verarbeitet dazu folgende Arten von Daten auf ihren Servern:

- PC-Name
- Betriebssystem
- Service Pack
- Gruppe, zu welcher der geschützte PC gehört
- Standard-IP-Adresse des Rechners
- MAC-Adresse
- IP-Adressen, die den verschiedenen Web-Adaptern zugewiesen werden
- MAC-Adressen für die verschiedenen Web-Adapter
- RAM-Speicher in MB

Wenn Sie CGM PROTECT EndPoint 360° nutzen, werden darüber hinaus Daten zum technischen Betrieb in der von unserem Vertragspartner WatchGuard Technologies, Inc., bereitgestellten Cloud mit Datenspeicherung in der EU verarbeitet. Es werden hierbei folgenden Daten im Rahmen der Kommunikation des Netzwerkes von und zum Internet erfasst:

- Trafficdaten aus dem Netzwerk der Einrichtung
- Countries
- Clients
- Domains
- URL Categories
- Destinations
- Applications
- Application Categories
- Protocols
- Malware Attacks
- Network Attacks
- Intrusion Prevention Service

Die vorgenannten technischen Daten werden stets innerhalb von 180 Tagen gelöscht.

3.3 Einsatz von Cookies

CGM PROTECT EndPoint 360° verwendet keine Cookies.

Weitere Tracking-Tools wie Pixel Tags, Google Remarketing etc. werden ebenfalls nicht verwendet.

3.4 Datenübermittlung

Für die Produktbereitstellung werden Daten in der von unserem Vertragspartner WatchGuard Technologies, Inc., USA, betriebenen Azure Cloud verarbeitet. Die eingesetzte Azure Cloud wird auf Servern in der EU gehostet. Diese Cloud bezieht WatchGuard Technologies, Inc. von

Microsoft Inc..Die Sie betreffenden Daten werden mithin nicht in die USA transferiert, sondern ausschließlich innerhalb der EU verarbeitet.

Daten in der Azure Cloud sind so verschlüsselt, dass weder WatchGuard Inc. noch Microsoft Inc. oder weitere Dritte Zugriff auf diese haben.

3.5 Verpflichtung auf Vertraulichkeit, Datenschutzschulungen

Patientendaten, insbesondere die Gesundheitsdaten, unterliegen neben den Sicherheitsanforderungen der Datenschutzgesetze (DS-GVO und BDSG neu), zusätzlich strengen Auflagen aus dem Strafgesetzbuch (StGB) sowie den Sozialgesetzbüchern (SGB) und werden von der CGM besonders sensibel behandelt.

Wir 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 (DS-GVO, §203 StGB) verpflichtend gebunden. Die Verletzung dieser Vertraulichkeitsverpflichtungen kann mit Kündigung und Strafverfolgung geahndet werden.

Die Mitarbeiter werden regelmäßig auf Datenschutz geschult.

4. Sicherheitsmaßnahmen / Vermeidung von Risiken

Die CGM trifft alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen, um Ihre personenbezogenen Daten sowie Ihrer 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.

5. 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**

  Zur Vorbeugung der Datenverluste werden die Daten regelmäßig gesichert.

- **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 auch jenseits der Konfiguration der Firewall auf Patienten- und Kundendaten und somit evtl. auch auf ihre Praxisdaten zurückgreifen müssen. Hierzu gibt es zentrale Regelungen der CGM.

  - 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. 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

6. Rechte der Betroffenen

Sie haben das Recht auf Auskunft über zu Ihrer Person gespeicherten Daten sowie ggf. Rechte auf Berichtigung, Einschränkung der Verarbeitung, Übertragung Ihrer Daten, 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.

Zur Geltendmachung Ihrer Rechte können Sie sich unter den nachstehenden Kontaktdaten an uns oder unseren Datenschutzbeauftragten wenden.

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.

7. 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.

8. 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.

9. Verantwortlich für CGM Deutschland AG

Vorstand / board of directors: Angela Mazza Teufer, Dr. Eckart Pech

CompuGroup Medical Deutschland AG
Maria Trost 21
56070 Koblenz

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

Hans Josef Gerlitz
CompuGroup Medical SE & Co KGaA
Maria Trost 21
D-56070 Koblenz
HansJosef.Gerlitz@CGM.com

10. Zuständige Aufsichtsbehörde

Für die CGM Medical Deutschland AG ist

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

als Aufsichtsbehörde zuständig.