Datenschutzerklärung der

CompuGroup Medical Deutschland AG – Geschäftsbereich Business Area Connectivity

1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Die Business Area Connectivity (nachfolgend BA Connectivity) erachtet den verantwortungsvollen Umgang und die Achtung des Schutzes personenbezogener Daten als obersten Grundsatz. Die BA Connectivity 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 SECURE WIFI.

Diese Datenschutzerklärung stellen wir als gemeinsam Verantwortliche mit den Leistungserbringern.

Die aktuelle Version dieser Datenschutzerklärung finden Sie immer unter https://cgm.com/protect-download.

2. CGM SECURE WIFI

CGM SECURE WIFI ist eine hochwertige technische Lösung zur sicheren Bereitstellung der angebundenen Netzwerke über WLAN mit hardwarebasierten Access Points. Die einzelnen Bestandteile werden dabei zentral verwaltet und bilden eine Einheit. Eine Netztrennung für Gast- und Patientenzugriffe kann rechtssicher und datenschutzkonform bereitgestellt werden und ist dabei von anderen Netzbereichen mit bewährter Technologie abgetrennt.

CGM SECURE WIFI 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

BA 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 Institution und BA Connectivity geschlossenen Vertragsverhältnisses. Zu diesen Daten gehören:

- Institutionsdaten
  - Institutionsname
  - Institutionstyp
  - Insitutions-Adresse
  - Telefonnummer
  - BSNR
  - NBSNR
- Arztdaten
  - Anrede / Titel
  - Vorname / Nachname
  - Namenszusatz
  - LANR
  - Fachrichtung

Des Weiteren optional hinzugefügt werden können:

- Geschlecht
- Geburtsdatum
- Land
- Telefon (privat)
- Telefon (mobil)
- Faxnummer
- Bankdaten (Einzugsermächtigung)
- E-Mail-Adresse
- Namen von Ansprechpartnern
- IP-Adresse bei Webshopbestellung

Im Rahmen der Vertrags- und Geschäftsbeziehung bekannt gewordene personenbezogene Daten werden von BA 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.

BA 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 Institutionsinhabers, nicht hingegen die von Ihnen in unseren Produkten abgespeicherte Daten Ihrer Patienten. Die CGM SE & Co.KGaA 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 BA 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

In manchen Fällen erhebt CGM-Daten zum technischen Betrieb, um die in einem Vertrag zugesicherten Leistungen bereitstellen zu können. Dies ist dann der Fall, wenn das Produkt oder ein zugehöriges Modul als Cloud-Produkt mit CGM-Hosting angeboten wird oder während einer Fernwartung. Im Übrigen 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.

Für die Nutzung von bei CGM gehosteten Cloud-Angeboten gelten die jeweiligen Beschreibungen für diese Cloud-Angebote. Näheres dazu finden Sie auch unter 4.3.

Die Daten zum technischen Betrieb werden auf dem Server der CGM in Deutschland gespeichert. Wir setzen dafür die CGM SE & Co. KGaA als Rechenzentrumsbetreiberin und Auftragsverarbeiterin datenschutzkonform ein.

Es werden folgende Daten gespeichert:

- Konfigurationsdaten der Access Points
- Seriennummer und IP-Adresse der Access Points
- Trafficdaten aus dem Netzwerk der Einrichtung
- Clients

Die vorgenannten technischen Daten, die in der WatchGuard Cloud verarbeitet werden, werden stets innerhalb von 180 Tagen gelöscht.

Konfigurationsdaten der Access Points werden persistent gespeichert.

3.3 Statistische Auswertungen, anonymisierte Daten

Es werden keine Daten für statistische Auswertungen verarbeitet.

3.4 Weitere Anwendungsfälle

Es werden keine Daten für andere Zwecke verarbeitet.

4. Verarbeitung von personenbezogenen Daten in CGM SECURE WIFI auf dem Server Ihrer Institution

Dieses Produkt wird nicht auf dem Server einer Institution installiert, bzw. es werden keine personenbezogenen Daten erfasst oder verarbeitet.

4.1 Stammdaten der Institution und der Institutionsmitarbeiter

Es werden keine personenbezogenen Daten erfasst oder verarbeitet.

4.2 Patientendaten

Es werden keine Patientendaten verarbeitet.

4.3 Verarbeitung von Institutionsdaten und besonderen Arten personenbezogener Daten |Patientendaten in integrierten Modulen

Es werden keine Patientendaten, besondere Arten personenbezogener Daten verarbeitet oder mit integrierten Modulen kommuniziert.

5. Datenübermittlung

Es werden keine Daten elektronisch auf gesetzlicher, vertraglicher oder einwilligungsbasierter Grundlage übermittelt.

6. 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.

7. 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.

8. Technische und organisatorische Maßnahmen

Die aktuelle Version der technischen und organisatorischen Maßnahmen finden Sie immer unter https://cgm.com/ti-download.

9. Durchführung von Online-Schulungen per Zoom und Microsoft Teams

Es finden keine Online-Schulungen per Zoom oder Microsoft Teams statt.

10. Nutzung von YouTube

Zu diesem Produkt gibt es keine YouTube Videos.

11. Online-Assistenten in CGM SECURE WIFI

Es werden keine Online-Assistenten genutzt.

12. Rechte der Betroffenen

Personenbezogene Daten des Arztes und der Institutionsmitarbeiter

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

Dieses Produkt speichert keine Patientendaten.

13. 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.

14. 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.

15. Verantwortlich für die BA Connectivity

Vorsitzender des Aufsichtsrates Prof. (apl.) Dr. med. Daniel Gotthardt
Vorstand Peter David

CompuGroup Medical Deutschland AG
Maria Trost 21
56070 Koblenz

16. 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

17. Zuständige Aufsichtsbehörde

Für die CGM Deutschland AG ist

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

als Aufsichtsbehörde zuständig.