

# Datenschutzerklärung der

## CompuGroup Medical Software GmbH – Geschäftsbereich CHS Consumer für das Produkt CGM CONNECT



### 1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Der Geschäftsbereich CHS Consumer erachtet den verantwortungsvollen Umgang und die Achtung des Schutzes personenbezogener Daten als obersten Grundsatz. CHS Consumer sichert stets die genaue Einhaltung aller relevanten Gesetze bei der Speicherung und Verarbeitung der personenbezogenen Daten zu.

CompuGroup Medical 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 CGM CONNECT.

Die aktuelle Version dieser Datenschutzerklärung finden Sie immer in CGM CONNECT selbst.

Die Datenschutzerklärung für die Internetpräsenz können folgenden Internetseiten entnommen werden:

[https://www.cgm.com/deu\\_de/system/datenschutzerklaerung.html](https://www.cgm.com/deu_de/system/datenschutzerklaerung.html)

### 2. Kommunikationstool CGM CONNECT

CGM CONNECT 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 den Zugriff auf bestimmte Module sowie die Regelung von Schreib- und Leserechten.

#### 2.1 CGM SMART UPDATE

CGM SMART UPDATE ist ein integriertes CGM CONNECT Plugin. Die Verwendung von CGM SMART UPDATE ist freiwillig. Nur, wenn Sie der Nutzung zustimmen, wird zur Laufzeit Ihre SAP ID, alte Kundennummer, BSNR, sowie die LANR erhoben und an den in Frankfurt bereitgestellten CGM Update Administrationsserver für die Authentifizierung übermittelt.

Folgende zusätzlichen Informationen werden von Ihren Endgeräten erhoben und im Administrationsserver in Frankfurt für einen besseren Kundensupport gespeichert:

- IP-Adresse
- MAC-Adresse
- Identifikations- ID des CGM SMART UPDATE (Finger Print)
- Festplattenkapazität
- RAM
- CPU
- Installierte Software
- GPU
- Betriebssystem
- Installierte AIS Version
- E-Mail-Adresse

Cloud Flare Inc. ist ein Unternehmen, welches Cloud Dienstleistungen anbietet. Cloud Flare Inc. nutzt für die Verteilung der Software ausschließlich Server in dem Land, aus welchem das Update angefordert wird. Dies dient einem beschleunigten Download. Dabei wird die IP-Adresse Ihres Anschlusses dem entsprechenden Server mitgeteilt und auch dort gespeichert. Die Löschung erfolgt automatisch nach einem Jahr. Eine in Deutschland ansässige Praxis wird demnach Updates nur aus Deutschland beziehen.

Die Verarbeitung und Speicherung erfolgen üblicherweise in Rechenzentren in der EU, sofern sich die Praxis in der EU aufhält. Sollte der unwahr-

scheinliche Fall eintreten, dass alle Cloud Flare Server in Deutschland ausfallen und das geografisch nächstgelegene Rechenzentrum sich außerhalb der EU befinden, weicht Cloud Flare bei der Verteilung von Updates auf Server in dem nächstliegenden Land aus. Wenn Sie die Lizenz Ihres AIS Produktes nicht verlängern und somit nicht mehr als Kunde der CGM geführt werden, werden die Daten auf dem Server automatisch gelöscht.

CGM SMART UPDATE verarbeitet keine Patientendaten.

### 3. Verarbeitung von personenbezogenen Daten durch CGM

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

Die CGM speichert bei der Verwendung der angebotenen Produkte / Dienste folgende Arten von Daten auf Ihren Server:

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

Wir verpflichten uns gemäß Datenschutzgesetz, sämtliche Vertragsdaten, sämtliche Protokolldaten und sämtliche Daten zum technischen Betrieb nach Kündigung Ihres Vertrages zu löschen.

Hierbei sind wir jedoch gesetzlich verpflichtet, Handels- und Steuerrechtliche Aufbewahrungsfristen zu beachten, die über die Dauer des Vertragsverhältnisses hinausgehen können. Daten zum technischen Betrieb werden nur so lange vorgehalten, wie es technisch notwendig ist, spätestens jedoch nach Kündigung Ihres Vertrages gelöscht.

#### 3.1 Vertrags- und Registrierungsdaten

Vertrags- und Registrierungsdaten dienen der Zuordnung und Betreuung eines zwischen der Praxis und CHS Consumer geschlossenen Vertragsverhältnisses. Zu diesen Daten gehören:

- Praxisdaten
  - Praxisname
  - Praxistyp
  - Praxis-Adresse
  - Telefonnummer
  - BSNR
  - E-Mail-Adresse
- Arztdaten
  - Anrede / Titel
  - Vorname / Nachname
  - Namenszusatz
  - LANR

Des Weiteren optional hinzugefügt werden können:

- Geschlecht
- Geburtsdatum
- Land
- Telefon (privat)
- Telefon (mobil)

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

# Datenschutzerklärung der

## CompuGroup Medical Software GmbH – Geschäftsbereich CHS Consumer für das Produkt CGM CONNECT



Nur bei vorliegender Einwilligung können diese Daten auch für produktbezogene Umfragen und Marketingzwecke genutzt werden.

Die Weitergabe, der Verkauf oder sonstige Übermittlung personenbezogener Daten an 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 CHS Consumer Anschrift und Bestelldaten bei Produktbestellung an Vertriebs- und Servicepartner weitergibt sowie die Anschrift an externe Produktionsfirmen zur Erstellung und dem Versand der Update-Datenträger.

Die Vertragsdaten werden auf dem CGM Server in Deutschland gespeichert.

Sie haben das Recht auf Auskunft über Ihre gespeicherten Daten, auf Berichtigung, Sperrung oder Löschung dieser Daten.

### 3.2 Daten zum technischen Betrieb

Daten zum technischen Betrieb werden benötigt, um die in einem Vertrag zugesicherten Leistungen bereitstellen zu können. Die CGM erhebt Daten zum technischen Betrieb nur zu diesem Zweck und überprüft regelmäßig, dass nur die Daten erhoben, gespeichert und verarbeitet werden, die notwendig sind, den technischen Betrieb ihrer Produkt-/Dienstleistungen bereitzustellen und zu verbessern.

Die Erhebung der Daten auf dem System der Praxis erfolgt nur, wenn Sie uns eine Einwilligung dafür erteilen.

Wenn Sie unsere Onlinedienste nutzen, werden zum Zweck der Systemicherheit temporär folgende Daten gespeichert:

- Domain-Namen,
- die IP-Adresse des anfragenden Rechners,
- das Zugriffsdatum bzw. den Zugriffszeitpunkt
- die Dateianfrage des Clients (Dateiname und URL),
- die Anzahl der im Rahmen der Verbindung transferierten Bytes.

Die Daten zum technischen Betrieb werden auf dem Server der CGM in Deutschland gespeichert. Daten, die während der Nutzung der Onlinedienste erhoben werden, werden innerhalb von 14 Monaten gelöscht. Die IP-Adressen werden in der Regel nicht gespeichert. Die Speicherung erfolgt nur, wenn Sie unsere Onlineupdates nutzen – hier wird sie aus Sicherheitsgründen überprüft.

### 3.3 Anonymisierte Daten

Wir anonymisieren individuelle Informationen und speichern sie auf einem separaten Server. Alle Daten, die von CHS Consumer erfasst werden, betreffen die Funktionalität der Software. Sie sind anonymisiert und können keinen Kunden zugeordnet werden.

## 4. Verarbeitung von personenbezogenen Daten in CGM CONNECT auf dem Server Ihrer Praxis

- **Stammdaten der Praxis und der Praxismitarbeiter**
- **Patientendaten**
  - **Stammdaten**
  - **Sensible Daten**

Diese Daten werden in der Datenbank auf dem Server Ihrer Praxis gespeichert und verarbeitet.

### 4.1 Stammdaten der Praxis und der Praxismitarbeiter

Die Speicherung von Stammdaten Ihrer Praxis ist insoweit notwendig, als dass diese für die Einhaltung gesetzlicher Vorschriften und zur korrekten Nutzung bestimmter Module/Verträge benötigt werden. Pflichtangaben zu Stammdaten sind in CGM CONNECT entsprechend gekennzeichnet. Zu den Stammdaten der Praxis und Praxismitarbeiter gehören Daten wie:

- Praxisname

- Praxistyp
- Praxisadresse
- BSNR
- Fachgebiet(e)
- E-Mail-Adresse
- Arztdaten
  - Anrede / Titel
  - Vorname / Nachname
  - Namenszusatz
  - LANR
- Weitere Mitarbeiter in der Praxis
  - Name
  - Vorname
  - Benutzerkürzel/Passwort

Stammdaten werden im Rahmen verschiedener Funktionen und Module benötigt und automatisch verwendet. Die Übertragung an Dritte erfolgt nach Zustimmung durch vorherige Einwilligung oder Benutzeraktion. Eine Berichtigung, Sperrung oder Löschung dieser Daten ist – unter Berücksichtigung der gesetzlichen Vorschriften- möglich. Beschreibungen zur Berichtigung, Sperrung oder Löschung finden Sie in den Einstellungen von CGM CONNECT unter dem Punkt "DSGVO".

## 4.2 Verarbeitung von Praxisdaten und besonderen Arten personenbezogener Daten | Patientendaten in integrierten Modulen

Integrierte Module werden zusammen mit CGM CONNECT standardmäßig installiert, interagieren mit diesem und verarbeiten im Funktionskontext personenbezogene Daten.

### Integrierte Module:

- **CGM ASSIST**

Der CGM Assist selbst speichert keine Patientendaten dauerhaft auf der Festplatte. Zur Laufzeit werden personenbezogene Daten in einer Memory-DB im Hauptspeicher der lokalen Instanz gespeichert. Wird der Prozess beendet, werden alle Daten im Hauptspeicher automatisch gelöscht.

- **CGM ASSIST eCockpit**

Das CGM Assist eCockpit selbst speichert keine Praxis- oder Patientendaten, sondern stellt zur Laufzeit eine View auf die von CGM CONNECT übergebenen Daten dar.

- **CGM ASSIST eCockpit-Verbindungstest-Tool**

Das CGM Assist eCockpit-Verbindungstest-Tool speichert Ergebnisse aus manuell aktivierten Verbindungstests. Gespeichert werden technische Daten des Verbindungstests wie Ergebnisse zur Erreichbarkeit von Servern und/oder IP-Adressen, Ports von verschiedenen Anwendungen/Services. Eine Löschung der Ergebnisse ist jederzeit möglich.

## 5. Datenübermittlung

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

### Zur elektronischen Übermittlung auf gesetzlicher Grundlage gehören

Datenübertragungen, die mittels folgender integrierter Services erfolgen:

- KV-Connect (sicherer und datenschutzkonformer Kommunikationskanal zwischen Leistungserbringern im Gesundheitswesen)
- Dale-UV (Übertragung von Unfallberichten an die DGUV)
- KIM (Kommunikation im Medizinwesen; ermöglicht den sicheren E-Mail- und Datenaustausch)

# Datenschutzerklärung der

## CompuGroup Medical Software GmbH – Geschäftsbereich CHS Consumer für das Produkt CGM CONNECT



Die Einhaltung der verpflichtenden Anforderungen der KBV zur sicheren Übertragung der Daten ist in CGM CONNECT gewährleistet.

### Zur elektronischen Übermittlung auf vertraglicher Grundlage gehören

- Sämtliche Daten, die gemäß HzV, Gevko, oder weiterer IV-/Versorgungsstruktur-Verträge in dem jeweiligen Anforderungskatalog für die Übermittlung spezifiziert sind- die Übermittlung erfolgt unter der Voraussetzung, dass der behandelnde Arzt und der Patient am Vertrag teilnehmen und damit ihre Einwilligung zum Verfahren gegeben haben. Dies sind Daten wie
  - Patiententeilnahmen
  - Abrechnungsdaten
  - Verordnungsdaten

Die Einhaltung der verpflichtenden Anforderungen zu Dateninhalten und Übertragungsweg gemäß der Anforderungskataloge zur sicheren Übertragung der Daten ist in CGM CONNECT gewährleistet.

### Elektronische Datenübermittlung aus weiteren einwilligungsbasierten Verfahren

Zu weiteren einwilligungsbasierten Verfahren gehören solche Funktionen, die nicht zu den gesetzlichen oder vertraglichen Verfahren gehören, wie

- Studien
- Übermittlung von Systemdaten an CGM

Hier erfolgt die Datenübermittlung auf Basis der transparenten Inhalte über den sicheren Übertragungsweg „CGM CONNECT“.

Zu „CGM CONNECT“: Während der Übermittlung wird der Übertragungsinhalt Ende-zu-Ende verschlüsselt. Während der Übermittlung wird der Transportinhalt mit einer Transportsignatur vor unbemerkter Veränderung geschützt.

Eine Übermittlung in Drittstaaten findet nicht statt.

## 6. Verpflichtung auf Vertraulichkeit, Datenschutzschulungen

Patientendaten, insbesondere die Gesundheitsdaten, unterliegen neben den Sicherheitsanforderungen der Datenschutzgesetze (DSGVO 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 (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 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.

## 8. Technische und organisatorische Maßnahmen

Um die Datensicherheit zu gewährleisten, überprüft die CGM regelmäßig den Stand der Technik. Hierzu werden unter anderem typische Schadensszenarien 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.

- 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

## Datenschutzerklärung der

CompuGroup Medical Software GmbH – Geschäftsbereich CHS Consumer für das Produkt  
CGM CONNECT



### 9. Rechte der Betroffenen

#### Personenbezogene Daten des Arztes und der Praxismitarbeiter

Sie haben das Recht auf Auskunft über zu Ihrer Person gespeicherten Daten sowie ggf. 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 der für Sie zuständigen Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Meinung sind, dass wir Ihre personenbezogenen Daten nicht richtig verarbeiten.

Wir verpflichten uns sämtliche Vertragsdaten, sämtliche Protokoll Daten und sämtliche Daten zum technischen Betrieb nach Kündigung Ihres Vertrages unaufgefordert zu löschen.

Hierbei sind wir jedoch gesetzlich verpflichtet, Handels- und steuerrechtliche Aufbewahrungsfristen zu beachten, die über die Dauer des Vertragsverhältnisses hinausgehen können. Daten zum technischen Betrieb werden nur so lange vorgehalten, wie es technisch notwendig ist, spätestens jedoch nach Kündigung Ihres Vertrages gelöscht.

#### Personenbezogene Daten Ihrer Patienten

Ihre Patienten haben das Recht auf Auskunft über zu ihnen gespeicherten Daten, 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 der für Sie zuständigen Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Meinung sind, dass Sie Ihre personenbezogenen Daten nicht richtig verarbeiten

### 10. 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.

### 11. 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 CompuGroup Medical SE & Co. KGaA oder CompuGroup Medical Deutschland AG.

### 12. Verantwortlich für die CHS Consumer

Herr Frank Brecher  
Herr 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 Auskunftersuchen oder Beschwerden Ihnen zur Verfügung steht

Hans Josef Gerlitz  
CompuGroup Medical SE & Co. KGaA  
Maria Trost 21  
D-56070 Koblenz  
[HansJosef.Gerlitz@CGM.com](mailto:HansJosef.Gerlitz@CGM.com)

### 13. Zuständige Aufsichtsbehörde

Für die CHS Consumer ist der  
Landesbeauftragte für den Datenschutz und die Informationsfreiheit  
Rheinland-Pfalz  
Hintere Bleiche 34  
55116 Mainz  
als Aufsichtsbehörde zuständig.