Datenschutzerklärung

der CompuGroup Medical Deutschland AG, Division Connectivity, Business Unit TI

Die CompuGroup Medical Deutschland AG (nachfolgend CGM genannt), freut sich über Ihr Interesse an unserem Produkt CGM KIM. Der Schutz Ihrer personenbezogenen Daten ist für die CGM ein wichtiges Anliegen. Nachfolgend stellen wir Ihnen vor, welche Informationen wir bei CGM bei der Nutzung des Produktes CGM KIM erfassen und wie diese verarbeitet werden.

Diese Datenschutzerklärung gilt ausschließlich für das **Produkt CGM KIM** (Kommunikation im Medizinwesen) der CompuGroup Medical Deutschland AG. Sie gilt nicht für eventuell vorhandene weiterführende Links zu fremden Unternehmen.

1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Der Geschäftsbereich Division Connectivity, Business Unit TI erachtet den verantwortungsvollen Umgang und die Achtung des Schutzes personenbezogener Daten als obersten Grundsatz und sichert stets die genaue Einhaltung aller relevanten Gesetze bei der Speicherung und Verarbeitung der personenbezogenen Daten ein.
CGM SE & Co. KGaA , als Mutterkonzern der CGM Deutschland AG, 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.

2. CGM KIM

Der neue Kommunikationsstandard Kommunikation im Medizinwesen (KIM) ermöglicht künftig eine barrierefreie, authentische und vertrauliche Kommunikation zwischen allen Leistungserbringern, Leistungserbringerinstitutionen, Kostenträgern und Interessenvertretern im deutschen Gesundheitswesen. Zwingende Voraussetzung: ein Anschluss an die Telematikinfrastruktur (TI). Dabei können sowohl Nachrichten und Dateien, als auch mittels elektronischem Heilberufsausweis oder der Praxis- bzw. Institutionskarte (SMC-B) signierte Dokumente über eine verschlüsselte E-Mail sicher über die TI ausgetauscht werden.

Mit dem Produkt CGM KIM kann der Kunde verschlüsselte und signierte Dokumente und Informationen sicher per E-Mail empfangen und versenden. Die Server für diese Kommunikation (z. B. Mailserver) werden in ISO-27001 zertifizierten Rechenzentren in Deutschland betrieben.

Der Versand und Empfang erfolgt direkt aus dem Primärsystem des Anwenders oder über einen marktüblichen E-Mailclient. Die Mail-Kommunikation erfolgt jederzeit über gesicherte Kommunikationswege in der TI, auf die unbefugte keinen Zugriff haben.

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

3. Erhebung und Verarbeitung von personenbezogenen Daten durch CGM

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Darunter fallen Informationen wie z.B. Ihr Name, Ihre Anschrift und Ihre Telefonnummer. Informationen, die nicht direkt mit Ihrer wirklichen Identität in Verbindung gebracht werden - wie z.B. bevorzugte Internetseiten oder Anzahl der Nutzer einer Seite - sind keine personenbezogenen Daten.

Die CGM speichert bei der Verwendung von CGM KIM folgende Arten von Daten auf Ihren Servern:

Daten zum technischen Betrieb des Produktes CGM KIM
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, um den technischen Betrieb ihrer Produkt-/Dienstleistungen bereitzustellen und zu verbessern.

Datenschutzerklärung

der CompuGroup Medical Deutschland AG, Division Connectivity, Business Unit TI

a) Clientmodul

Für den Versand aus der Institution erhebt und verarbeitet das CGM KIM-Clientmodul in der Institution personenbezogene Daten. Das Clientmodul kommuniziert als zentrale Komponente mit dem Clientsystem/Primärsystem und dem Konnektor. Die Kommunikation zwischen den Komponenten erfolgt von Clientsystem zum Clientmodul und von Clientmodul zu Konnektor jederzeit über verschlüsselte Verbindungen (TLS).

Das CGM KIM-Clientmodul erhebt und verarbeitet die vom Clientsystem/Primärsystem übergebenen Daten (z. B. medizinische Daten, personenbezogene Daten, KIM-Adresse des Versenders und Empfängers,…) je nach Anwendungsfall in der KIM-Nachricht oder als Nachrichten-Anhang. Die Daten liegen dem Clientmodul, nach der Übertragung über eine gesicherte Verbindung, bis zur Übergabe zur Signierung und Verschlüsselung an den Konnektor im Klartext vor. Für die Verifizierung des KIM-Accounts am CGM KIM-Fachdienst verarbeitet das Clientmodul die vom Clientsystem per TLS übermittelten Login-Daten.

Im Rahmen einer Suchanfrage an den Verzeichnisdienst (KIM-Adressbuch) übergibt das anfragende Clientsystem die Daten an den Konnektor, der die Anfrage an den Verzeichnisdienst weitergibt. Bei dieser durchgehend verschlüsselten Kommunikation kann je nach Abfrage Name, Titel, Fachgebiet, Organisation, Straße, Hausnummer, PLZ, Ort, Bundesland erhoben und verarbeitet werden.

Die Kommunikation zwischen CGM KIM-Clientmodul und CGM KIM-Fachdienst erfolgt verschlüsselt über die sicheren E-Mail-Protokolle SMTPS und POP3S. Die vom Konnektor signierten und verschlüsselten Nachrichten werden verschlüsselt auf dem CGM KIM-Fachdienst abgelegt. Die Nachrichten sind ausschließlich vom Empfänger über das private Zertifikat der SMC-B oder des eHBA abruf- und entschlüsselbar.

b) CGM KIM Assist

Der CGM KIM Assist ist die clientseitige Komponente zur Einrichtung und Verwaltung des CGM KIM Accounts. Im Rahmen der Einrichtung des CGM KIM Accounts werden die folgenden Daten zur Prüfung angezeigt jedoch nicht gespeichert und, falls noch nicht durch den Identitätsprovider der SMC-B/des HBA geschehen, werden die Daten durch den Anwender vervollständigt und an den Verzeichnisdienst in der TI übertragen:

Telematik-ID, Name, Titel, Fachgebiet, Organisation, Betriebsstättennummer (BSNR), Straße, Hausnummer, PLZ, Ort, Bundesland

c) Fachdienst

Der CGM KIM-Fachdienst ist die serverseitige Komponente in der KIM-Kommunikation. Im Rahmen von CGM KIM verarbeitet und erhebt der CGM KIM-Fachdienst folgende personenbezogenen Daten:

- Registrierungs- und Deregistrierungsdaten:
  AUT-Zertifikat, KIM-Adresse und die dazugehörigen Login-Daten

- Login-Daten:
  Für den Login des Users verarbeitet der CGM KIM-Fachdienst den vom Clientmodul übergebenen Benutzernamen und Passwort für die Verifizierung des Anwenders an seinem Postfach. Die Übertragung von Benutzername und Passwort erfolgt stehts über eine beidseitig gesicherte TLS Verbindung.

- Basisdaten zur Nutzung des CGM KIM-Fachdienstes:
  Telematik-ID, Name, Titel, Fachgebiet, Organisation, Betriebsstättennummer (BSNR), Straße, Hausnummer, PLZ, Ort, Bundesland, CGM KIM-Adresse.

Jegliche Kommunikation vom Fachdienst mit dem VZD ist beidseitig über TLS gesichert.

- Protokolldaten:
  Siehe Punkt "4. Protokollierung"

- Verkehrsdaten:
  Siehe Punkt "4. Protokollierung"

Folgende Daten sind nicht Gegenstand der Verarbeitung innerhalb des Fachdienstes:

- Inhaltsdaten:
  Nachrichteninhalte, hochgeladene und empfangene Dateien und Dokumente

Die Daten werden auf den Servern der CGM, gemäß gematik Spezifikationen, in Deutschland gespeichert. Daten, die während der Nutzung von CGM KIM erhoben werden, werden innerhalb von 90 Tagen gelöscht.

4. Protokollierung

a) Serverseitige Protokollierung

Die CGM installiert für die Nachvollziehbarkeit von Vorgängen am KIM-Fachdienst Maßnahmen und Verfahren gemäß DSGVO i. V. m. BDSG.

Die CGM protokolliert dabei folgende Informationen:

- Anmeldung von Nutzern (KIM-Adresse, Nutzername und Uhrzeit)

- Informationen über empfangene, weitergeleitete und abgeholte Nachrichten, Absender, Empfänger, Datum und Uhrzeit des Zugriffs bzw. der Zustellung, Größe und Anzahl der KIM-Nachrichten

- Fehlermeldungen (Fehler mit Beschreibung und Uhrzeit) mit Fehler, Fehlerbeschreibung, Uhrzeit und eindeutige Referenznummer

Die im Rahmen der Nachrichtenverarbeitung erzeugten Logfiles werden nach 90 Tagen gelöscht.

Zum Zwecke der Fehler- bzw. Störungsbehebung protokolliert die CGM im KIM-Fachdienst unter Berücksichtigung des Art. 25 Abs. 2 DSGVO nur Protokolldaten entsprechend dem Datenschutzgrundsatz nach Art. 5 DSGVO. Die Protokolldaten enthalten personenbezogene Daten in der Art und dem Umfang, wie sie zur Behebung von Fehlern und Störungen erforderlich sind. Die erzeugten Protokolldaten im KIM-Fachdienst werden nach der Behebung unverzüglich gelöscht.

b) Clientseitige Protokollierung

CGM KIM-Clientmodul/CGM KIM-Assist

Zum Zwecke der Fehler- bzw. Störungsbehebung protokolliert das CGM KIM-Clientmodul und der CGM KIM-Assist Abläufe, Performanceinformationen, Fehler, Fehlerbeschreibung, Uhrzeit und eine eindeutige Referenznummer, jedoch keine medizinischen oder personenbezogenen Daten sowie kein geheimes Schlüsselmaterial oder Passwörter.

Nur autorisierte Personen haben Zugriff auf diese Daten, die nach 30 Tage gelöscht werden. Die Protokollierung kann im Falle der Fehler- bzw. Störungsbehebung von einer autorisierten Person eingesehen werden. CGM hat keinen Zugriff auf diese lokal abgelegten Daten. Der Zugriff durch die CGM auf diese Daten kann ausschließlich über einen vom Anwender autorisierten Zugang (z. B. per Fernwartung oder vor Ort) ermöglicht werden.

5. Verpflichtung auf Vertraulichkeit und Datenschutzschulungen

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.

6. Technische und organisatorische Maßnahmen

Um die Datensicherheit zu gewährleisten, verpflichtet sich die CGM, dem jeweiligen technischen Entwicklungsstand entsprechend Vorkehrungen zu treffen, um die Einhaltung der relevanten Datenschutzbestimmungen zu gewährleisten.
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 Penetrationstests zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen zur Gewährleistung der sicheren 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 (Institution / 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 Daten Ihrer Kunden zurückgreifen müssen. Hierzu gibt es zentrale Regelungen der CGM:

- Die Fernwartungs-Zugänge bleiben geschlossen und werden nur durch den Kunden freigeschaltet.
- Passwörter zu Kundensystemen werden nur für die Fernwartung erteilt.
- Besondere Tätigkeiten werden durch das Vier-Augen-Prinzip 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 Kundenverwaltungssystem der CGM. Dokumentiert werden: Ausführender Mitarbeiter, Zeitpunkt (Datum/Uhrzeit), Tätigkeit, Dauer, Zielsystem, das Fernwartungsmedium, kurze Beschreibung der Tätigkeit.
- Bei kritischen Tätigkeiten werden auch die nach dem als Vier-Augen-Prinzip herangezogenen Mitarbeiter erfasst.
- Die Aufzeichnung der Sitzungen ist verboten

7. Durchsetzung

Die CGM überprüft regelmäßig und durchgängig die Einhaltung dieser Datenschutzerklärung. 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. Sicherheitsmaßnahmen / Vermeidung von Risiken

Die CGM trifft alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen, um Ihre personenbezogenen Daten vor unerlaubtem Zugriff, unerlaubten Änderungen, Offenlegung, Verlust, Vernichtung und sonstigen Missbrauch zu schützen. So werden Ihre Daten in einer sicheren Betriebsumgebung gespeichert, die der Öffentlichkeit nicht zugänglich ist.
In bestimmten Fällen werden Ihre personenbezogenen Daten bei der Übermittlung durch die sog. Secure Socket Layer-Technologie (SSL) verschlüsselt. Das bedeutet, dass die Kommunikation zwischen Ihrem Computer und den Servern von CGM unter Einsatz eines anerkannten Verschlüsselungsverfahrens erfolgt, wenn Ihr Browser SSL unterstützt.
Die CGM prüft intern die Vorgehensweisen bei der Datenerhebung, -speicherung sowie -verarbeitung und setzt weiterhin Sicherheitsmaßnahmen zum Schutz vor unberechtigtem Zugriff auf Systeme ein, auf denen Vertragsdaten oder Daten zum technischen Betrieb gespeichert werden.

9. Rechte der Betroffenen

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

Bei der CGM erteilten Einwilligung 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.

Wir verpflichten uns gemäß Datenschutzgesetz sämtliche Vertragsdaten, Protokolldaten, Registrierungsdaten, bestellbezogene 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.

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 Datenschutzerklärung ist anhand ihres Daten- und Versionsstandes zu identifizieren.

Verantwortlich für die Division Connectivity,

Vorstand: Frank Brecher, Dr. Eckart Pech
CompuGroup Medical Deutschland AG
Maria Trost 21
56070 Koblenz

Datenschutzerklärung

der CompuGroup Medical Deutschland AG, Division Connectivity, Business Unit TI

11. Datenschutzbeauftragter

Bei Fragen hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten können Sie sich an den Datenschutzbeauftragten der CompuGroup Medical SE & Co. KGaA wenden, der Ihnen im Falle von Auskunftsersuchen oder Beschwerden zur Verfügung steht:

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

Zuständige Aufsichtsbehörde

Für die Division Connectivity, Business Unit TI ist

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

Als Aufsichtsbehörde zuständig.