Datenschutzerklärung der

CompuGroup Medical Deutschland AG – Business Area Connectivity

1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Die Business Area Connectivity erachtet den verantwortungsvollen Umgang und die Achtung des Schutzes personenbezogener Daten als obersten Grundsatz. Die Business Area 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 bei der CGM im Zusammenhang mit dem Einsatz von einem Produkt zur Verfügung, so dass auch Sie Ihre Patienten und Kunden entsprechend informieren können. Diese Datenschutzerklärung bezieht sich auf den CGM TI-Messenger.

Diese Datenschutzerklärung stellen wir als Produkthersteller zur Information über unsere Produkte zur Verfügung.

Die aktuellste Version dieser Datenschutzerklärung finden Sie immer unter https://www.cgm.com/deu_de/plattformen/telematikinfrastruktur/downloads.html sowie im CGM TI-Messenger selbst.

2. CGM TI-Messenger

Der CGM TI-Messenger ermöglicht eine sichere Echtzeit-Kommunikation im deutschen Gesundheitswesen zwischen allen an die Telematikinfrastruktur (TI) angeschlossenen Organisationen. Relevante Informationen und Dateianhänge können mit dem CGM TI-Messenger sicher, schnell und unkompliziert ausgetauscht werden. Der CGM TI-Messenger wird ähnlich zu bekannten Instant-Messengern verwendet, jedoch mit dem Vorteil, dass er die notwendige Datenschutzkonformität für das Gesundheitswesen mitbringt. Jede Kommunikation über den CGM TI-Messenger ist Ende-zu-Ende verschlüsselt und somit vor dem Zugriff durch Dritte geschützt. Durch die Entwicklung auf Basis eines sicheren Messenger-Standards nach gematik-Vorgabe wird ein sektoren- und anbieterübergreifender Austausch möglich.

3. Verarbeitung von personenbezogenen Daten durch CGM

Die Business Area Connectivity speichert bei der Verwendung der angebotenen Produkte / Dienste Vertrags- und Registrierungsdaten und Daten zum technischen Betrieb auf ihren Servern.

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.

Information zum primären Zweck der Anwendung und die Verwendung von personenbezogenen Daten werden bei der erstmaligen Nutzung im Rahmen der vom Nutzer zu bestätigenden Nutzungsbedingungen angezeigt.

Die Anwendung erhebt und verarbeitet ausschließlich Daten, die dem primären Zweck der Anwendung dienen. Dabei ist der primäre Zweck der Anwendung die Verarbeitung von CGM TI-Messenger Nachrichteninhalten, die Ende-zu-Ende-verschlüsselt übermittelt werden. Dies sind Nutzerdaten zur Verwaltung und Anzeige von Absendern und Empfängern nach gematik-Spezifikation, Kommunikationsinhalte sowie im Rahmen des Matrix-Protokolls benötigte Raum- und Metadaten. Diese Daten (Raum- und Metadaten) enthalten Informationen über das versendete Dokument oder die Nachricht. Sie sind nicht der Hauptinhalt, sondern geben den Kontext dazu. Beim CGM TI-Messenger ist dies z. B. die Information, ob ein Chatraum ein privater Chatraum oder ein öffentlicher Chatraum ist.

3.1 Vertrags- und Registrierungsdaten

Vertrags- und Registrierungsdaten dienen der Zuordnung und Betreuung eines zwischen Ihnen und Business Area Connectivity geschlossenen Vertragsverhältnisses. Zu diesen Daten gehören:

- KIM-Adresse
- Domainname/n des CGM TI-Messengers der Organisation
- Kundennummer
- Webshop-ID / Kunden-ID

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

Die Business Area Connectivity arbeitet mit der CGM arbeitsteilig in gemeinsamer Verantwortlichkeit für die Bereitstellung von IT für die Kundenkommunikation, das Kundencontrolling, Finance, Marketing und Kundensupport zusammen. Hierbei werden u. U. auch personenbezogene Kundendaten verarbeitet, beispielsweise der Name eines Praxisinhabers, nicht dagegen von Ihnen in unseren Produkten abgespeicherte Daten. Die CGM stellt in diesen Bereichen die Tools bereit. Wir melden unsere Bedarfe und nutzen die Tools. Über diese Datenverarbeitung in gemeinsamer Verantwortlichkeit haben wir mit der CGM einen Vertrag geschlossen mit folgendem wesentlichen Inhalt gem. Art. 26 Abs. 2 DSGVO: 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 als Rechenzentrumsbetreiberin und Auftragsverarbeiterin datenschutzkonform ein. Die Vertragsdaten werden nach einer Aufbewahrungszeit von 10 Jahren nach Vertragsende vollständig gelöscht.

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, wenn dies zum Zwecke der Vertragsabwicklung erforderlich ist oder eine ausdrückliche Einwilligung vorliegt. Es kann beispielsweise erforderlich sein, dass die Business Area Connectivity Anschrift und Bestelldaten bei Produktbestellung an Dienstleister vor Ort (DVO) weitergibt.

3.2 Daten zum technischen Betrieb

CGM erhebt Daten zum technischen Betrieb, um die zugesicherten Leistungen bereitstellen zu können.

Die detaillierten Informationen sind in Kapitel 4 beschrieben.

4. Verarbeitung von personenbezogenen Daten im CGM TI-Messenger

Der CGM TI-Messenger verarbeitet Daten in ISO-27001 zertifizierten Rechenzentren der CGM in Deutschland.

Zu diesen Daten gehören Stammdaten der Organisation und der Mitarbeiter der Organisation,

- Name der Organisation
- Organisationstyp
- Adresse der Organisation
- Fachgebiet(e)
- Daten der verantwortlichen Person der Organisation
    - Anrede / Titel
    - Vorname / Nachname
    - Anzeigename
    - Namenszusatz
    - E-Mail-Adresse
    - Matrix-ID
- Weitere Mitarbeiter in der Organisation (weitere CGM TI-Messenger Nutzer)
    - Name
    - Vorname
    - Anzeigename
    - E-Mail-Adresse
    - Matrix-ID
- KIM-Adresse
- Telematik-ID
- Domainname/n des CGM TI-Messengers der Organisation
- Kundennummer
- Webshop-ID / Kunden-ID

Authentisierungstoken, kryptographische Identitäten,
CGM TI-Messenger Metadaten

- Pushdaten, die dazu verwendet werden den Nutzer über neue Nachrichten zu informieren
- Daten, die zur Aktualisierung des Präsenzstatus notwendig sind,
- Daten, die zur Aktualisierung des Lesestatus notwendig sind

und Protokolldaten bzw. Logdaten.

4.1 Stammdaten der Organisation und der Mitarbeiter

Der Abruf von Stammdaten Ihrer Organisation aus dem Verzeichnisdienst (VZD) der gematik ist insoweit notwendig, da diese für die Anzeige in der Oberfläche des CGM TI-Messengers z. B. in der Administrationsoberfläche benötigt werden.
Für die Nutzung des CGM TI-Messengers wird eine Authentifizierung jedes Nutzers vorausgesetzt. Die CGM stellt hierfür die sogenannte CGM ID zur Verfügung, die zur Anmeldung am CGM TI-Messenger verwendet wird. Weitere Infos zum Datenschutz der CGM ID finden Sie unter https://id.cgm.com/docs/gdpr_de.pdf.

Der bei der CGM ID angegebene Vorname und Nachname wird per default als sog. Anzeigename für die Kommunikation im CGM TI-Messenger festgelegt. Dieser kann durch den Administrator der Organisation geändert werden. Der Displayname ist notwendig, um den durch die gematik aufgrund des gesetzlichen Auftrags spezifizierten Leistungsumfang zu erbringen und den Empfänger und Sender einer Nachricht zu identifizieren.

Die E-Mail-Adresse zur Anlage der CGM ID wird initial zur Identifikation des Nutzers abgerufen, aber im CGM TI-Messenger nicht weiterverwendet.

Jeder Nutzer wird nach initialer Anlage einer CGM ID und beim ersten Zugriff auf den CGM TI-Messenger auf die in der CGM ID angegebenen und vom CGM TI-Messenger genutzten Daten hingewiesen und muss separat die Zustimmung erteilen.

Die KIM-Adresse, Domainname des CGM TI-Messengers der Organisation und die CGM-Kunden-IDs wie z.B. Kundennummer sowie Webshop-ID werden für die Herstellung der technischen Funktionsfähigkeit genutzt und um die korrekte Identifizierung des Vertragspartners zu gewährleisten.

Stammdaten der Organisation und der Organisationsmitarbeiter werden während des Betriebes des CGM TI-Messengers gespeichert und verarbeitet und spätestens 30 Tage nach Vertragsende unwiderruflich gelöscht.

4.2 Authentisierungstoken, kryptographische Identitäten

Diese Daten dienen der Authentisierung der Nutzer und damit der Gewährleistung der Vertraulichkeit während des Betriebs des CGM TI-Messengers. Sie sind für die Funktionsfähigkeit nach gematik-Spezifikation zwingend erforderlich.

Authentisierungstoken und kryptographische Identitäten stellen eine Pseudonymisierung der Nutzeridentität dar. Eine weitergehende Anonymisierung ist nicht möglich, da die Daten zur eindeutigen Identifizierung benötigt werden. Die technische Löschung eines Nutzers erfolgt 30 Tage nach Löschung durch den Administrator der Organisation außerhalb der Verantwortung der CGM oder automatisch nach spätestens 30 Tagen nach Ablauf des Vertrags und Beendigung der Nutzung des CGM TI-Messengers.

4.3 CGM TI-Messenger Metadaten

CGM TI-Messenger Metadaten werden z. T. nur nach expliziter Zustimmung verarbeitet (z. B. Setzen des Anzeigenamens, Aus- und Anschalten von Präsenz- und Lesestatus) und von der CGM nicht dauerhaft gespeichert.

Diese Metadaten sind notwendig, um den durch die gematik aufgrund des gesetzlichen Auftrags spezifizierten Leistungsumfang zu erbringen. CGM TI-Messenger Metadaten wie z. B. Benachrichtigungen von Nachrichtenempfängern über die Übermittlung von Pushdaten sind zur Gewährleistung einer zeitnahen Kommunikation und den prozessualen Ablauf des CGM TI-Messengers erforderlich.

4.4 Protokolldaten bzw. Logdaten

Zur Nachvollziehbarkeit der Verwendung des CGM TI-Messengers, zur Gewährleistung der Verfügbarkeit und zur Sicherstellung der technischen Funktionsfähigkeit werden Logdaten protokolliert. Es findet keine Protokollierung der CGM TI-Messenger-Nachrichteninhalte statt. Aufgrund der eingesetzten Ende-zu-Ende-Verschlüsselung der CGM TI-Messenger-Nachrichten verfügt CGM zu keinem Zeitpunkt über die Möglichkeit, auf die Nachrichteninhalte zuzugreifen.

Eine Speicherung erfolgt gemäß den Vorgaben der gematik für Protokolldaten zur Fehler- bzw. Störungsbehebung nur bis zum Abschluss der Fehlerbehebung. Unter Berücksichtigung des Art. 25 Abs. 2 DSGVO wird sichergestellt, dass in den Protokolldaten entsprechend dem Datenschutzgrundsatz nach Art. 5 DSGVO nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind und dass die erzeugten Protokolldaten im CGM TI-Messenger nach der Behebung unverzüglich gelöscht werden. Sofern andere gesetzliche Grundlagen wie § 331 SGB V nicht überwiegen werden hierzu nur anonymisierte Daten protokolliert.

5. Datenübermittlung

Der CGM TI-Messenger übermittelt Daten elektronisch auf vertraglicher oder einwilligungsbasierter Grundlage nur nach Interaktion durch den Nutzer oder – nach erteilter Zustimmung- automatisiert.

Die Verantwortung für die Transparenz zur Nutzung des CGM TI-Messengers liegt bei der jeweils nutzenden Organisation. Aufgrund der eingesetzten Ende-zu-Ende-Verschlüsselung der CGM TI-Messenger-Nachrichten verfügt CGM zu keinem Zeitpunkt über die Möglichkeit, auf die Nachrichteninhalte zuzugreifen.

Die CGM hat zu keinem Zeitpunkt Einsicht auf die übermittelten Inhalte, da die Inhalte clientseitig ver- und entschlüsselt werden.

Die Gewährleistung der weitergehenden Verarbeitung liegt in Drittsystemen z. B. zur Archivierung (insb. zur Erfüllung gesetzlicher Anforderungen).

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 der 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 nach Art. 6 Abs. 1 (a), (b) und (c) DSGVO 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. Rechte der Betroffenen

Personenbezogene Daten der Organisation und der Organisationsmitarbeiter

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.

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.

11. Verantwortlich für die Business Area Connectivity

CompuGroup Medical Deutschland AG
Maria Trost 21
56070 Koblenz

info.ti@cgm.com

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

12. 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.