

# Systemvoraussetzungen

Version 2025.12

**CompuGroup Medical Deutschland AG**

Maria Trost 21, 56070 Koblenz

T +49 (0) 261 8000-0

[info.de@cgm.com](mailto:info.de@cgm.com)

[cgm.com/de](http://cgm.com/de)

# Inhaltsverzeichnis

---

<b>Allgemeine Informationen für den Betrieb von CGM Praxis .....</b>	<b>4</b>
<b>IT-Sicherheit .....</b>	<b>5</b>
Allgemeine Empfehlungen zur IT-Sicherheit .....	5
Betriebssysteme .....	5
Web-Browser .....	6
Firewall- und Port-Einstellungen .....	6
Besondere Module zur IT-Sicherheit .....	6
An- und Abmeldung .....	6
Externe Softwarelösungen .....	7
Schlussfolgerung .....	7
<b>Hardwareanforderungen .....</b>	<b>8</b>
Arbeitsplatz-Computer .....	8
Mindestanforderungen .....	8
Empfohlene Hardware .....	8
Arbeitsplatz-Monitor .....	8
Mindestanforderungen .....	8
Empfohlene Einstellung .....	8
Ausfallsicherheit .....	9
<b>Netzwerk .....</b>	<b>10</b>
Internetanbindung .....	10
Mindestanforderungen: .....	10
<b>Geräte-Anbindung .....</b>	<b>11</b>
Medizinische elektrische Geräte .....	11

---

Kartenterminals (falls erforderlich) .....	11
<b>Betriebssysteme (alle 64-Bit) .....</b>	<b>12</b>
Arbeitsstationen .....	12
Mindestanforderungen: .....	12
Empfohlene Ausstattung: .....	12
Service Pack (Microsoft) .....	12
Support-Ende .....	12
<b>Unterstützte Browser .....</b>	<b>13</b>
<b>Installation .....</b>	<b>14</b>
<b>Datensicherung .....</b>	<b>15</b>
<b>Datensicherheit .....</b>	<b>16</b>
Verschlüsselung .....	16
<b>Änderungshistorie .....</b>	<b>17</b>

## **Allgemeine Informationen für den Betrieb von CGM Praxis**

CGM Praxis ist ein Arztinformationssystem mit einer großen Funktionsvielfalt. Um diese optimal nutzen zu können, bedarf es gewisser technischer Voraussetzungen (Hardware). Damit Sie CGM Praxis vollumfänglich in Ihren Praxisalltag integrieren und von allen Funktionen profitieren können, orientieren Sie sich bitte an den folgenden Systemanforderungen.

# IT-Sicherheit

Die Gewährleistung von IT-Sicherheit und Datenschutz ist in der Medizinbranche von größter Bedeutung. CGM Praxis verpflichtet sich zu höchsten Sicherheitsstandards, um die sensiblen Daten von Patienten und Praxen zu schützen. Dieses Kapitel gibt allgemeine Empfehlungen zur IT-Sicherheit sowie spezielle Hinweise zu den Sicherheitsmodulen der CompuGroup Medical Deutschland AG, den PC Log-In-Funktionen, den Betriebssystemen, Firewall- und Port-Einstellungen und externen Softwarelösungen.

## Allgemeine Empfehlungen zur IT-Sicherheit

- **Regelmäßige Updates:** CGM Praxis wird als Cloud-Software regelmäßig mit Updates versorgt. Halten Sie zusätzlich das Installationsprogramm „CGM PRAXIS Arbeitsplatzinstallation“ (notwendig zur eindeutigen Identifizierung von Arbeitsplätzen und zur Anbindung von Druckern etc.) stets auf dem neusten Stand. Halten Sie außerdem das zugrundeliegende Betriebssystem und Ihren Web-Browser stets auf dem neuesten Stand. Installieren Sie alle verfügbaren Updates zeitnah, um Sicherheitslücken zu schließen und neue Funktionen zu nutzen.
- **Starke Passwörter:** Verwenden Sie komplexe Passwörter mit mindestens 10 Zeichen, die aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Vermeiden Sie leicht zu erratende Passwörter und ändern Sie diese regelmäßig. Ändern Sie Standardpasswörter auf allen Geräten und Systemen unverzüglich nach der Einrichtung.
- **Zugriffsrechte:** Weisen Sie Benutzern nur die benötigten Zugriffsrechte zu. Nutzen Sie die Möglichkeit, Rollen und Berechtigungen in CGM Praxis zu definieren, um Datenzugriffe zu steuern.
- **Sicherheitsbewusstsein:** Schulen Sie alle Mitarbeiter regelmäßig in Bezug auf IT-Sicherheit und Datenschutz. Sensibilisieren Sie sie für Phishing-Angriffe und andere Bedrohungen. Ziehen Sie auch gerne unsere „Liste bekannter Schwachstellen“ zurate, unter **Menü > Hilfe & Informationen > Produktinformationen**. Hier werden potenzielle Schwachstellen aufgeführt, inklusive Handlungsempfehlungen.
- **Datensicherung:** Die CGM Praxis-Datenbank wird automatisch gesichert. Bei weiteren Fragen wenden Sie sich an Ihren CGM Praxis-Support.

## Betriebssysteme

- **Unterstützte Betriebssysteme:** Stellen Sie sicher, dass Sie eine [unterstützte Version des Betriebssystems](#) verwenden (z. B. Windows 11). Überprüfen Sie regelmäßig die Kompatibilität mit der neuesten Version von CGM Praxis.
- **Sicherheitseinstellungen:** Aktivieren Sie die integrierten Sicherheitsfunktionen des Betriebssystems, wie z. B. Windows Defender, um zusätzlichen Schutz vor Malware und Viren zu gewährleisten.

## Web-Browser

- **Unterstützte Web-Browser:** Stellen Sie sicher, dass Sie eine [unterstützte Version des Web-Browsers](#) verwenden (z. B. Google Chrome). Überprüfen Sie regelmäßig die Kompatibilität mit der neuesten Version von CGM Praxis.

## Firewall- und Port-Einstellungen

- **Firewall-Regeln:** Aktivieren Sie die Firewall Ihres Betriebssystems und konfigurieren Sie sie so, dass verdächtige Verbindungen blockiert werden. Erstellen Sie spezifische Firewall-Regeln, um den Netzwerkzugriff auf CGM Praxis zu kontrollieren.
- **Port-Einstellungen:** Schließen Sie alle nicht benötigten Ports, um unautorisierte Zugriffe zu verhindern. Prüfen Sie regelmäßig die offenen Ports auf Ihrem System und passen Sie die Einstellungen gegebenenfalls an.
- **Netzwerküberwachung:** Implementieren Sie Werkzeuge zur Überwachung des Netzwerkverkehrs, um ungewöhnliche Aktivitäten zu erkennen. Dies hilft, potenzielle Sicherheitsvorfälle frühzeitig zu identifizieren.
- **Incident Response Plan/ Vorfalldaktionsplan:** Seien Sie auf potenzielle Sicherheitsvorfälle vorbereitet, indem Sie einen klaren Reaktionsplan erstellen. Dieser Plan sollte definieren, wie schnell und effektiv auf Sicherheitsverletzungen reagiert wird. Legen Sie Verantwortlichkeiten, Kommunikationswege und konkrete Maßnahmen zur Schadensbegrenzung fest, um im Ernstfall handlungsfähig zu bleiben.

## Besondere Module zur IT-Sicherheit

- **Security Monitoring/ Sicherheitsüberwachung:** CGM Praxis nutzt ein integriertes Monitoring-Tool zur Überwachung von ungewöhnlichen Aktivitäten und Sicherheitsvorfällen. Dies umfasst die Protokollierung von Zugriffen und Änderungen innerhalb der Software.
- **Verschlüsselung:** Alle sensiblen Daten werden sowohl bei der Speicherung als auch bei der Übertragung durch moderne Verschlüsselungstechniken geschützt.
- **Antiviren-Integration:** Integrieren Sie eine zuverlässige Antivirensoftware, die in Echtzeit Sicherheitsbedrohungen erkennt und blockiert. Halten Sie diese Software stets auf dem neuesten Stand.

## An- und Abmeldung

- **Sichere Anmeldeverfahren:** Verwenden Sie zwingend die Zwei-Faktor-Authentifizierung (2FA) beim Login in die CGM Praxis-Software. Dies erhöht die Sicherheit erheblich und schützt vor unbefugtem Zugriff.

- **Automatische Abmeldung:** Aktivieren Sie auch auf Ihrem lokalen Endgerät die Funktion zur automatischen Abmeldung nach einer festgelegten Inaktivitätszeit. Dies verhindert, dass unbefugte Personen Zugriff auf Ihr System erhalten, wenn ein Benutzer seinen Arbeitsplatz verlässt. CGM Praxis hat diese Funktion standardmäßig aktiviert.

## Externe Softwarelösungen

- **Zuverlässige Software:** Verwenden Sie nur vertrauenswürdige externe Softwarelösungen, die den Datenschutzerfordernissen entsprechen. Informieren Sie sich über die Sicherheitszertifikate und Datenschutzrichtlinien der jeweiligen Anbieter.
- **Integration von Drittanbietersoftware:** Stellen Sie sicher, dass integrierte Drittanbietersoftware (z. B. Praxisverwaltungssysteme, Abrechnungssoftware) ebenfalls sicher konfiguriert ist. Überprüfen Sie die Kompatibilität mit CGM Praxis und halten Sie diese Software ebenfalls regelmäßig auf dem neuesten Stand.
- **Datenschutzbestimmungen:** Beachten Sie stets die datenschutzrechtlichen Bestimmungen und stellen Sie sicher, dass die externe Software die notwendigen Maßnahmen zum Schutz sensibler Patientendaten umsetzt.

## Schlussfolgerung

Die Implementierung der oben genannten Empfehlungen und Module ist entscheidend für die Sicherheit Ihrer Praxisdaten und die Einhaltung der gesetzlichen Vorgaben. CGM Praxis unterstützt Sie dabei, Ihre IT-Sicherheitsstrategie zu optimieren. Bei Fragen oder Unterstützung wenden Sie sich bitte an Ihren zuständigen Vertriebs- und Servicepartner.

Informieren Sie sich gerne auch zu den Sicherheitsempfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) z. B. durch deren [Newsletter](#).

# Hardwareanforderungen

Es werden jeweils minimale und empfohlene Systemanforderungen beschrieben. Die minimalen Systemanforderungen stellen die untere Grenze für ein lauffähiges System dar. Aus diesem Grund verweisen wir hier auf die empfohlenen Systemanforderungen und raten Ihnen, diese Variante einzusetzen, damit ein performantes Arbeiten in der Praxis ermöglicht wird.

## Arbeitsplatz-Computer

### Mindestanforderungen

- Prozessor:  
  
Windows: Dual-Core Prozessor (Intel i5, 1,8 GHz o.ä.) oder höher  
  
Mac: 64-Bit Intel oder Apple Silicon ARM
- Arbeitsspeicher: 4 GB oder mehr (davon mind. 150 MB frei)
- Festplatte: 150 MB freier Speicherplatz (Wenn die Hilfsanwendung für TI, Kartenleser-Funktion und Drucken/Scannen installiert ist)

### Empfohlene Hardware

- Prozessor:  
  
Windows: Dual-Core Prozessor (Intel i5, 1,8 GHz o.ä.) oder höher  
  
Mac: 64-Bit Intel oder Apple Silicon ARM
- Arbeitsspeicher: 8 GB oder mehr (davon mind. 400 MB frei)
- Festplatte: 200 MB freier Speicherplatz (Wenn die Hilfsanwendung für TI, Kartenleser-Funktion und Drucken/Scannen installiert ist)

## Arbeitsplatz-Monitor

### Mindestanforderungen

Auflösung mindestens 1920 x 1080 Pixel.

### Empfohlene Einstellung

Auflösung Full-HD 1920 x 1080 Pixel oder höher.

## **Ausfallsicherheit**

Sollte Ihr CGM Praxis wider Erwarten ausfallen, prüfen Sie bitte zunächst Ihre Internetverbindung. Wenn hier keine Einschränkungen vorliegen, wenden Sie sich bitte an Ihren CGM Praxis-Support.

# Netzwerk

## Internetanbindung

Internetzugang ist auf allen Arbeitsplatzrechnern erforderlich. Eine Backup-Internetleitung, insbesondere über ein anderes Medium als das Hauptinternet (z. B. über einen Mobilfunkanbieter), wird empfohlen.

### Mindestanforderungen:

- 16 Mbit/s Downstream oder schneller

# Geräte-Anbindung

## Medizinische elektrische Geräte

Sämtliche Computerarbeitsplätze, die an ein Medizinprodukt angeschlossen sind und dadurch - direkt oder indirekt - Patientenkontakt haben ( z. B. Audiometer, EKG, EEG, Lungenfunktion, Sonographie-Geräte, Endoskopie-Gerät, Perimeter, Phoropter u. a.), müssen den Anforderungen der IEC 60601-1 "Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale" entsprechen. Die Einhaltung dieser Norm gewährleistet die grundlegende elektrische Sicherheit und die Erfüllung der relevanten Leistungsanforderungen für alle angebundenen medizinischen Systeme.

## Kartenterminals (falls erforderlich)

Für die Nutzung eines Kartenterminals (zum Einlesen von Versichertenkarten) ist ein per USB-Kabel verbundenes Kartenlesegerät nötig. Hierfür muss der entsprechende USB Port Device Driver (CT-API-kompatibel) installiert werden.

## Betriebssysteme (alle 64-Bit)

CGM Praxis ist für die unten folgenden Betriebssysteme geprüft und zugelassen.

Für erhöhte Sicherheit und optimale Leistung empfehlen wir die Verwendung eines gehärteten Betriebssystems beim Betrieb von CGM Praxis. Bitte beziehen Sie sich auf die offiziellen Microsoft-Richtlinien zur Betriebssystem-Härtung [windows-security-baselines](https://support.microsoft.com/de-de/windows-security-baselines) sowie die offiziellen Apple-Richtlinien <https://support.apple.com/de-de/guide/security/seccd5016d31/1/web/1> und <https://support.apple.com/de-de/100100> .

## Arbeitsstationen

### Mindestanforderungen:

- Windows 11 (64-Bit)
- macOS 14.5 Sonoma

### Empfohlene Ausstattung:

- Windows 11 (64-Bit)
- macOS 15 Sequoia

## Service Pack (Microsoft)

Anlehndend an die Aussage von Microsoft endet der Support eines Service Packs 24 Monate nach Erscheinen der nächsten Service Pack-Version.

## Support-Ende

Alle zugelassenen Microsoft-Betriebssysteme und -Versionen werden bis zum Ablauf des „Mainstream Support“ von Microsoft unterstützt.

<https://docs.microsoft.com/de-de/lifecycle/>

Alle zugelassenen MAC-Betriebssysteme und -Versionen werden bis zum End-of-Support unterstützt, in der Regel 3 Jahre nach dem Erscheinungsdatum.

<https://support.apple.com/de-de/100100>

## Unterstützte Browser

Für die optimale Nutzung von CGM Praxis empfehlen wir für die Nutzung am Desktop folgende Browser:

- Google Chrome 85+
- Microsoft Edge 139+

## Installation

Für die Installation des Installationsprogramms „CGM PRAXIS Arbeitsplatzinstallation“ (notwendig zur eindeutigen Identifizierung von Arbeitsplätzen und zur Anbindung von Druckern etc.) sind Administratorrechte notwendig.

## Datensicherung

Die CGM Praxis-Datenbank wird automatisch gesichert. Bei weiteren Fragen wenden Sie sich an Ihren CGM Praxis-Support.

# Datensicherheit

## Verschlüsselung

Alle sensiblen Daten werden sowohl bei der Speicherung als auch bei der Übertragung durch moderne Verschlüsselungstechniken geschützt. Der automatisierte Prozess zum Backup der Datenbank wird jährlich im Rahmen des Audits für Backup und Wiederherstellung getestet. Vollständige Backups werden in einem verschlüsselten S3-Bucket mit einer Aufbewahrungsfrist von 14 Tagen gespeichert.

## Änderungshistorie

Version	Datum	Änderung	Autor
1.0	09.07.2025	Erstellung des Dokuments.	Sophie Schäfer
2.0	22.08.2025	Freigabe Browser Microsoft Edge 139+	Sophie Schäfer
3.0	23.10.2025	Änderung Kapitel "Medizinische elektrische Geräte"	Sophie Schäfer

# CGMone | Praxis

**CompuGroup Medical Deutschland AG**

Maria Trost 21, 56070 Koblenz

T +49 (0) 261 8000-0

[info.de@cgm.com](mailto:info.de@cgm.com)

[cgm.com/de](http://cgm.com/de)