

# Technische und organisatorische Maßnahmen zum Datenschutz und Datensicherheit

Zentrales Datenschutzmanagement Standort Martinsried  
ifap Service-Institut für Ärzte und Apotheker GmbH  
Bunsenstrasse 7 | 82152 Martinsried / München

## 1. Vertraulichkeit

---

(Art. 32 Abs. 1 lit. b DS-GVO)

### Zutrittskontrolle

#### Sicherungsmaßnahmen des Gebäudes / des Betriebsgeländes Martinsried

Folgende Sicherungsmaßnahmen des Betriebsgeländes und der Gebäude bestehen.

#### **Überwachung der Gebäude und des Betriebsgeländes**

Die Gebäude werden überwacht durch:

- Gebäude-Alarmanlage mit Verbindung zu Feuerwehr
- Externen Wachdienst
- Intern akustischer Alarm

Das Betriebsgelände wird überwacht durch:

- Wachdienst mit Rundgängen

#### **Sicherung und Zugang zum Betriebsgelände**

Der Haupteingang zum Betriebsgelände ist geöffnet in der Zeit von 6:00 Uhr bis 20:00 Uhr. Direkter Zutritt zum Firmengelände ist nur Mitarbeitern gestattet. Gäste werden von den entsprechenden Mitarbeitern am Empfang entgegengenommen und dürfen sich nicht frei auf dem Gelände bewegen. Alle Gäste werden im zentralen Besucherbuch eingetragen. Außerhalb der Öffnungszeiten können autorisierte Personen Zutritt zum Gelände über einen entsprechenden Schlüssel erlangen.

#### **Schließsystem Gebäude- Eingangstür/en**

Alle Gebäudeeingänge verfügen über ein zentrales Schließsystem.

#### **Andere Zu- und Ausgänge**

Weitere Zu- und Ausgänge zu den Gebäuden befinden sich in

- Tiefgarage (extra gesichert)
- Keller (extra gesichert)

## Sicherungsmaßnahmen innerhalb der Geschäftsräume

### Zutritt zu den Geschäftsräumen, Serverräumen, Archivräumen, usw.

Im Gebäude sind mehrere Firmen ansässig. Die Geschäftsräume sind permanent verschlossen. Der Zutritt zu allen Geschäftsräumen wird mittels

- Mitarbeiterausweise inkl. Zutrittssicherung
- Schlüssel

kontrolliert.

Räume der Datenverarbeitung verfügen über einen separaten Schließkreis (Schlüssel).

Die Arbeitsplätze der System-Administration befinden sich in einem separaten und mit Zugangskontrollsystem versehenen Bereich des Gebäudes.

### Organisatorische Regelungen über Zutrittsberechtigungen

Organisatorische Regelungen über Zutrittsberechtigungen zu Geschäftsbereichen werden mittels Dienstanweisungen geregelt.

### Verwaltung der Zutrittsmittel

Zur Verwaltung der Zutrittsmittel existiert eine Dienstanweisung. Diese regelt auch die Dokumentation der Zutrittsmittel.

Maßnahmen/Regelungen bei Verlust eines Zutrittsmittels sind ebenfalls in der Dienstanweisung festgeschrieben.

### Zutritte sonstiger Personen in die Geschäftsräume

Dritte haben die Möglichkeit von 8:00 bis 16:00 Uhr über den Empfang (begleitet) in die Geschäftsräume zu gelangen. Dritte müssen sich am Empfang in ein Protokollbuch eintragen.

### Reinigung der Geschäftsräume

Die Geschäftsräume werden durch einen externen Dienstleister gereinigt. Für Räume, die verschlossen sind, ist der jeweilige Mitarbeiter verantwortlich.

### Zutritt zum Rechenzentrum

Die Datenverarbeitungstechnik ist auf dem Betriebsgelände in dedizierten Räumen untergebracht. Das Rechenzentrum ist permanent mit einbruchs- und feuerhemmenden Türen verschlossen. Zutritt ist nur über autorisierte Personen mittels separatem Schlüssel möglich.

### Sicherungsmaßnahmen in den Räumlichkeiten

Geschäftsräume sind mit Isolierverglasung versehen.

Räume mit Datenverarbeitungsanlagen besitzen keine Fenster.

## Sicherungsmaßnahmen des Gebäudes / des Betriebsgeländes Standort Koblenz

Folgende Sicherungsmaßnahmen des Betriebsgeländes und der Gebäude bestehen:

### **Überwachung der Gebäude und des Betriebsgeländes**

Die Gebäude werden überwacht durch:

- Bewegungsmelder
- Videoüberwachung
- Gebäude-Alarmanlage mit Verbindung zu
- Externem Wachdienst
- Intern Akustischer Alarm

Das Betriebsgelände wird überwacht durch:

- Wachdienst mit Rundgängen

### **Sicherung und Zugang zum Betriebsgelände**

Das komplette Betriebsgelände ist mit einem Gittermattenzaun (2m Höhe) umgeben. Der Haupteingang zum Betriebsgelände ist geöffnet in der Zeit von 7:30 Uhr bis 19:00 Uhr. Direkter Zutritt zum Firmengelände ist nur Mitarbeitern gestattet. Gäste werden von den entsprechenden Mitarbeitern an der Pforte in Empfang genommen und dürfen sich nicht frei auf dem Gelände bewegen. Alle Gäste werden im zentralen Besucherbuch eingetragen und tragen sichtbar Benutzerausweise. Außerhalb der Öffnungszeiten der Pforte können autorisierte Personen Zutritt zum Gelände über eine Magnetkarte oder entsprechenden Schlüssel erlangen.

### **Schließsystem Gebäude- Eingangstür/en**

Alle Gebäudeeingänge verfügen über ein zentrales Schließsystem.

### **Andere Zu- und Ausgänge**

Weitere Zu- und Ausgänge zu den Gebäuden befinden sich in

- Tiefgarage (extra gesichert)
- Dachluke
- Balkone
- Keller (extra gesichert)
- Dachterrassen

Dachluke, Balkone und Dachterrassen sind ohne Hilfsmittel nicht zu erreichen.

### **Zugang zum Rechenzentrum**

Die Datenverarbeitungstechnik ist auf dem Betriebsgelände in dedizierten Räumen untergebracht. Das Rechenzentrum ist permanent mit einbruchs- und feuerhemmenden Türen verschlossen. Zutritt ist nur über autorisierte Personen mittels 2-Faktor Autorisierung (Zutrittskontrollsystem, PIN) möglich. Der Zugang des Rechenzentrums wird permanent mit Kameras überwacht.

## Sicherungsmaßnahmen des Gebäudes / des Betriebsgeländes Rechenzentrum Frankfurt

Folgende Sicherungsmaßnahmen des Betriebsgeländes und der Gebäude bestehen:

### **Überwachung der Gebäude und des Betriebsgeländes**

Die Gebäude werden überwacht durch:

- Alarmanlage
- Gebäudebewachung
- Videoüberwachung

Das Betriebsgelände wird überwacht durch:

- Sicherheitsdienst (24h/7 Tage)
- Durchgängig besetzter Empfang im Verwaltungsgebäude

### **Sicherung und Zutritt zum Betriebsgelände**

Das gesamte Gelände ist von einem Sicherheitszaun umgeben.

Die Zufahrt zum Gelände ist nur über eine beschränkte Pforte möglich.

Das Rechenzentrum/die Serverräume befinden sich in einem separat gesicherten und überwachten Gebäude.

Zutritt haben nur die Mitarbeiter (abgestufte Zutrittsregelungen). Der Zutritt muss unabhängig von den vorhandenen Ausweisen im Vorfeld angemeldet werden.

Es werden Anwesenheitsaufzeichnungen im Sicherheitsbereich geführt

Es bestehen schriftliche Zutrittsregelungen.

Der Zutritt für grundsätzlich nicht zugriffsberechtigter Mitarbeiter und unternehmensfremder Personen (z. B. Wartungstechniker, Reinigungskräfte, Besucher) ist durch Begleitung geregelt.

Der Zutritt zu DV- und TK-Systemen wird Unbefugten durch folgende Maßnahmen verwehrt:

- Automatische Zutrittskontrolle
- Berechtigungsausweis
- Biometrische Prüfung
- Vereinzelungsanlage

Elektronische Zutrittssicherung im Verwaltungsgebäude

### **Zutritt zum Rechenzentrum**

Die Datenverarbeitungstechnik ist auf dem Betriebsgelände in dedizierten Räumen untergebracht. Das Rechenzentrum ist permanent mit einbruchs- und feuerhemmenden Türen verschlossen. Zutritt ist nur über autorisierte Personen mittels 2-Faktor Autorisierung (Berechtigungsausweis + Biometrische Prüfung) möglich. Der Zugang des Rechenzentrums wird permanent mit Kameras überwacht.

## Zugangskontrolle zu Datenverarbeitungsanlagen

Mit der Zugangskontrolle soll die Benutzung der Datenverarbeitungsanlage/n gesichert werden. Zunächst betrifft dies den lokalen Zugangsschutz, wie z.B. passwortgesicherter Zugang auf Betriebssystemebene oder chipkartengeschützter Zugang. Bei vernetzten Systemen muss der Zugang zusätzlich gegen Zugriffe über das Netz geschützt werden. Insbesondere bei Anschluss an das Internet sind erhöhte Anforderungen an den Schutz zu stellen. Eine Sicherung hat i.d.R. über Firewall usw. zu erfolgen.

### Arbeitsplatzgestaltung

Die eingerichteten Arbeitsplätze sind in den Bereichen, in denen Besucher Zugang haben, so gestaltet, dass Externen kein Einblick (Bildschirm, Drucker, Fax, usw.) auf personenbezogene Daten geboten wird.

### Identifikation und Authentifikation von Benutzern

Identifikation und Authentifikation von Benutzern erfolgt mit User-ID und Passwort am Client sowie an der Anwendung/Host (abhängig von der Applikation). Nach 15 Minuten Inaktivität des Benutzers wird die Bildschirmsperre des Arbeitsplatzrechners erzwungen. Die Bildschirmsperre ist nur durch Eingabe des Passwortes aufhebbar.

### Single-Sign-On / Durchreichen des Login-Passwortes

Anwendungssysteme verwenden Single-Sign-On mittels Durchreichen des Passwortes an die Anwendung/Host.

### Passwortrichtlinien

Es existieren Vorgaben für die Mindestlänge und Komplexitätsanforderungen von Passwörtern. Passwörter sind mit einer Gültigkeitsdauer und Zahl von Generationen versehen.

Die dargestellten Passwortkonventionen werden durch Systemeinstellungen erzwungen.

### Remotezugriff von Mitarbeitern

Remotezugriff von Mitarbeitern erfolgt ausschließlich über Dienstrechner der Mitarbeiter sowie über verschlüsselte VPN-Verbindungen. Die Dienstrechner sind mit einem aktuellen Virenschutz versehen. Jeder Remotezugriff muss beantragt werden und unterliegen der Genehmigung. Die genehmigten Anträge werden von der CGM GroupIT aufgenommen und dokumentiert. Pro Antrag wird ein zeitlich begrenztes Zertifikat generiert. Die Einrichtung des Remotezugriffs erfolgt durch den Client-Service der CGM GroupIT.

### Wartungs- und Reparaturarbeiten

Wartungs- und Reparaturarbeiten werden von externen Unternehmen durchgeführt. Es erfolgt eine Beaufsichtigung durch fachkundige Mitarbeiter.

Für wiederkehrende Maßnahmen liegt ein Fristenplan für Wartungsarbeiten vor.

Werden IT-Systeme außer Haus gegeben, werden zuvor alle sensitiven Daten, die sich auf

Datenträgern befinden physikalisch gelöscht.

Die mit der Reparatur beauftragten Unternehmen werden auf die Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen verpflichtet.

## Zugriffskontrolle zu Datenverarbeitungssystem

Zu verstehen ist hier insbesondere die Kontrolle der Berechtigung zum Zugriff auf die jeweiligen Daten. Nur die Person, die den Zugriff auf jeweilige Daten für ihre jeweilige Tätigkeit benötigt, darf die Zugriffsrechte erhalten. Es wird gewährleistet, dass die Nutzungsberechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

### Systemadministration CGM

Die Administration der Datenverarbeitungssysteme wird von internen Mitarbeitern der CGM SE durchgeführt.

Administratoren identifizieren sich mit User-ID und Passwort gegen den Client und ggf. die Anwendung/Host.

Für die Differenzierung zwischen der User- (ein Account) und Administrationstätigkeit (bis zu zwei Accounts für unterschiedliche Berechtigungsstufen) werden separate User-ID / Passwort pro Person eingesetzt.

## Trennungskontrolle

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und zwar durch eine logische oder physikalische Trennung.

## 2. Integrität

---

(Art. 32 Abs. 1 lit. b DS-GVO)

### Weitergabekontrolle/Aufbewahrung/Vernichtung

Ziel ist die Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Datenweitergabe und –transport beruht auf einheitlichen Systemen zur Authentifizierung von Benutzern durch Benutzererkennung, Zertifikat und Passwort.

Alle Kanäle über unsichere Medien werden mittels kryptographischer Verschlüsselung (VPN) gesichert.

Datenträger, die aus Gründen der Betriebssicherheit angefertigt werden, werden an zentralen Stellen unter Verschluss gehalten (im Sicherheitsbereich + Tresor).

Datenträger werden aus Gründen der Betriebssicherheit zusätzlich an einem externen Standort ausgelagert.

Es existieren Regelungen über die Vernichtung von Datenträgern/Festplatten etc. (z. B. Anzahl der Löschvorgänge).

Nicht mehr benötigte Dokumente in Papierform werden in den Bereichen geschreddert. Dokumente, die personenbezogene Daten beinhalten, werden in Schreddern mit Sicherheitsstufe nach DIN 66399 Stufe P-3 bzw. P-4 geschreddert. Entsorgung von größeren Mengen der Dokumente erfolgt über ein zertifiziertes Drittunternehmen.

### Eingabekontrolle

Je nach Verhältnismäßigkeit wird die revisionssichere automatische Protokollierung der Eingaben in Logfiles oder Tabellen erzwungen. Elemente der Protokollierung sind:

- betroffener Datensatz
- Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes)
- Zeitpunkt der Aktivität bzw. des Ereignisses
- ausführende Person (Benutzerkennzeichen)

Je nach Notwendigkeit wird eine Auswertungsmöglichkeit dieses Protokolls zur Verfügung gestellt.

## 3. Verfügbarkeit und Belastbarkeit

---

(Art. 32 Abs. 1 lit. b DS-GVO)

### Verfügbarkeitskontrolle

#### Betriebsbereitschaft Koblenz und Rechenzentrum Frankfurt

Der Betrieb wird durch Personal vor Ort von 8:00 Uhr bis 18:00 Uhr, Montag bis Freitag sichergestellt. Die IT-Systeme werden rund um die Uhr mittels einer Überwachungslösung überwacht. Es existiert ein Alarmierungsplan.

#### Datensicherung Standort Koblenz

- Es findet eine tägliche automatisierte Sicherung der Daten im Rechenzentrum statt
- Es werden Kopien der Datensicherungen ausgelagert
- Es erfolgt eine tägliche Prüfung der Protokollierung der Datensicherung.
- Jeden Monat wird ein Einleseversuch der Datensicherung unternommen.
- Jedes Jahr wird eine Wiederherstellung durchgeführt.

#### Datensicherung Rechenzentrum Frankfurt

- Es findet eine tägliche automatisierte Sicherung der Daten im Rechenzentrum statt
- Es erfolgt eine tägliche Prüfung der Protokollierung der Datensicherung.
- Jedes Jahr wird eine Wiederherstellung durchgeführt.

#### Unterbrechungsfreie Stromversorgung / Notstromaggregat

Alle systemrelevanten Datenverarbeitungsanlagen sind mit einer ausreichend dimensionierten USV versehen. Das Rechenzentrum verfügt über ein Notstromaggregat. Dieses wird regelmäßig gewartet und einmal monatlich betrieben.

Im Rechenzentrum in Frankfurt sind auch ÜberspannungsfILTER eingebaut und es erfolgt eine Temperatur- und Feuchtigkeitsüberwachung.

### Wiederherstellbarkeit

Es findet mindestens einmal jährlich ein Wiederherstellungstest für jede Geschäftseinheit innerhalb des Konzerns statt. Die zeitliche Planung u. Einteilung der Wiederherstellungstests wird von der zentralen IT-Abteilung (CGM GroupIT) gesteuert u. nach den in der unternehmensweit gültigen Datensicherungsrichtlinie (Global Backup Policy) beschriebenen Kriterien durchgeführt. Die Ergebnisse der Wiederherstellungstests werden dokumentiert. Es gibt einen definierten Eskalationsprozess, welcher sicherstellen soll, dass Fehler u. Probleme die bei Durchführung des Tests eingetreten sind, zeitnah behoben werden.

Die Richtlinie Global Backup Policy umfasst unter anderem Prozesse u. Definitionen zu

- Zeitplanung, Art u. Umfang der Recovery Tests
- verwendete interne u. externe Schnittstellen mit Verantwortlichkeiten



- Risikobewertung der eingesetzten Prozesse
- Beschreibung Eskalationsprozess u. Maßnahmenplan

## Richtlinien zur Datensicherheit

### Vorliegende Richtlinien/Anweisungen

- Geeignete IT-Sicherheitsmaßnahmen (Datensicherungskonzept)
- Sicherheits- und Notfallkonzept
- IT-Sicherheitsanforderungen
- Förderung des Sicherheitsbewusstseins (z.B. der Mitarbeiter)
- Zur Langzeit-Archivierung
- Nutzung von E-Mail
- Nutzung von Internet
- Schutz, Bekanntgabe und Vernichtung von Daten
- Sicherheitsleitlinien für Mitarbeiter

### Regelmäßige Aktivitäten

- Wartung von Sicherheitseinrichtungen
- Administrativer Support von Sicherheitseinrichtungen
- Reaktion auf sicherheitsrelevante Ereignisse
- Fortlaufende Überwachung der IT-Systeme
- Change Management
- Überprüfung von Maßnahmen auf die Übereinstimmung mit der Sicherheitspolitik
- Mitarbeiterschulungen

### Weitergehende Maßnahmen

- Basis-Benutzerpasswort
- Mehrfach-Log-ons und –Passwörter
- Single-Sign-On-Software
- Virtual Private Network (VPN) für Datenverschlüsselung
- Secure Sockets Layer (SSL)
- Spam-Filter
- Paket-Filter
- Content-Filter
- Desktop-Antiviren-Software
- Gateway-Antiviren-Software
- Personal-Firewalls
- Anwendungs-Firewalls
- Netzwerk-Firewalls
- VPN-Lösung für Homeoffice-Anbindung

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

---

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

### Datenschutzmanagement

Das Datenschutz-Managementsystem ist ein Instrument zur Einhaltung von Datenschutzbestimmungen. CGM führte bereits 2012 ein zentrales Datenschutzmanagement ein.

In das Datenschutzmanagement sind die Vorstände und alle General Manager als Verantwortliche sowie beratend und regulatorisch der Datenschutzbeauftragte und die Datenschutzkoordinatoren als Erfüllungsgehilfen des Datenschutzbeauftragten eingebunden. In jeder Business Unit (BU) der CGM ist ein Datenschutzkoordinator benannt. Aufgaben und Pflichten des Datenschutzbeauftragten und der Datenschutzkoordinatoren sind in einer Verfahrensanweisung definiert. Die Bestellung erfolgt formal und anhand einer standardisierten Vorlage.

#### Der Beauftragte für den Datenschutz (DSB) und Datenschutzkoordinatoren (DSK)

Der Beauftragte für den Datenschutz als internes fachlich weisungsunabhängiges Organ überwacht die Einhaltung der Datenschutzvorschriften. Er ist verantwortlich für die Richtlinien auf dem Gebiet des Datenschutzes und überwacht deren Einhaltung. Er führt Datenschutz-Kontrollen und -Audits durch. Der Beauftragte für den Datenschutz wird vom Vorstand der CGM SE bestellt und betreut zentral alle deutschen Unternehmen des Konzerns.

Die jeweiligen General Manager benennen dem Beauftragten für den Datenschutz pro BU einen Datenschutzkoordinator. Die Datenschutzkoordinatoren sind vor Ort Ansprechpartner für den Datenschutz. Sie können in Abstimmung mit dem Beauftragten für den Datenschutz Kontrollen durchführen und haben die Inhalte der Datenschutzrichtlinien den Mitarbeitern bekannt zu machen. Die Geschäftsbereichsleiter sind verpflichtet, den Beauftragten für den Datenschutz und die Datenschutzkoordinatoren in ihrer Tätigkeit zu unterstützen.

Die Mitarbeiter der Bereiche, die personenbezogene Daten verarbeiten, werden im erforderlichen Umfang im Umgang mit personenbezogenen Daten geschult. Der Beauftragte für den Datenschutz stellt dafür ein webbasiertes Schulungstool zur Verfügung. Die Verantwortung für die Durchführung Schulungen liegt in den Fachbereichen. Die Schulungen finden jährlich statt, neue Mitarbeiter werden unmittelbar nach der Einstellung geschult. Zertifikate werden in den Personalakten der Mitarbeiter abgelegt.

Bei der geplanten Einführung oder Änderung von Verfahren zur Verarbeitung personenbezogener Daten (z. B. Einführung neuer Soft- oder Hardware, Einschaltung externer Dienstleister, Weitergabe von Daten an andere CGM Unternehmen, Nutzung von Shared Services) werden die Datenschutzkoordinatoren bzw. der Beauftragte für den Datenschutz frühzeitig vorab eingebunden.

Bei Datenverarbeitungsvorhaben, aus denen sich Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, wird der Beauftragte für den Datenschutz schon vor der Einführung der Verarbeitung beteiligt. Dies gilt insbesondere für besonders schutzbedürftige personenbezogene Daten.

Bei Datenschutzverletzungen und Beschwerden sind die verantwortlichen Führungskräfte durch definierte Prozesse verpflichtet, umgehend den Beauftragten für den Datenschutz zu

unterrichten. Daneben kann sich jeder Betroffene jederzeit mit Anfragen oder an den Beauftragten für den Datenschutz wenden. Die Anfragen und Beschwerden werden vertraulich behandelt. Die Empfehlungen des Beauftragten für den Datenschutz zur Abhilfe der Datenschutzverletzung sind durch die jeweiligen Geschäftsführungen und Geschäftsbereichsleiter bei der Entscheidung zu berücksichtigen.

Der Datenschutzbeauftragte berichtet an den Vorstand der CGM und die General Manager der jeweiligen BU. Die regelmäßige Berichtserstattung erfolgt wöchentlich in Schriftform und je zwei Monate als Präsenzbericht. Dazwischen werden anlassbezogene Berichte erstattet.

Die Datenschutzkoordinatoren berichten anlassbezogen an den Datenschutzbeauftragten und General Manager.

### Verantwortlichkeiten und Sanktionen

Die Verantwortlichkeiten sind in den internen Regelungen der CGM und in den Prozessbeschreibungen definiert.

Die Vorstände der CGM SE und General Manager der Konzern-Unternehmen der CGM SE sind für die Beachtung der gesetzlichen und den in den internen Datenschutzrichtlinien, Verfahrens- und Fachanweisungen formulierten Anforderungen und Regelungen des Datenschutzes verantwortlich. Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine rechtskonforme Datenverarbeitung unter Beachtung des Datenschutzrechtes in ihrem Verantwortungsbereich sicherzustellen.

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen.

Zu widerhandlungen, für die einzelne Mitarbeiter verantwortlich gemacht werden können, ziehen grundsätzlich arbeitsrechtliche Sanktionen entsprechend dem geltenden Recht bezogen auf diese Personen nach sich.

### Datenschutz-Regelungen

Die Datenschutz-Regelungen der CGM sind zentral, d.h. sie gelten für alle Unternehmen im Konzern. Bestimmte Abweichungen werden nur dann zugelassen, wenn die zentralen Regelungen dadurch nicht beeinträchtigt werden und nur in Abstimmung mit dem Datenschutzbeauftragten.

Die Datenschutz-Regelungen sind in Form von ISO-Dokumenten verfasst und bilden ein Teil des gesamten QM-Regelwerkes der CGM.

Als Zentrales Dokument für den Datenschutz gilt die Konzernrichtlinie zum Datenschutz. Sie beinhaltet alle allgemeinen Regeln und Definitionen sowie definiert die Struktur des zentralen Datenschutzmanagements der CGM.

Von der Konzernrichtlinie zum Datenschutz werden Verfahrensanweisungen abgeleitet. Sie regeln konkrete Vorgänge und Abläufe, definieren die Verantwortlichkeiten dafür und schreiben Dokumentationspflichten vor. Falls notwendig, definieren sie auch weitere, verfahrensbezogene technische und organisatorische Maßnahmen. Folgende Vorgänge sind durch diese Regelungen abgedeckt:

- Informationspflichten des Unternehmens
- Gewährung der Rechte der Betroffenen
- Umgang mit Kunden und Patientendaten (inkl. Fernwartung und Datenimporte)

- Datenschutz-Folgenabschätzung
- AV Verträge
- Datenpannen

Die Verfahrensanweisungen werden durch weitere Hilfsmittel wie Checklisten und Vorlagen begleitet.

Jede BU kann von den Verfahrensanweisungen eigene Fachanweisungen ableiten. Eine Fachanweisung ist eine Schritt-für-Schritt Anweisung zur Umsetzung einer Verfahrensanweisung.

Alle Dokumente sind zentral abgelegt.

Neben den verpflichtenden Datenschutzregelungen wurden bestimmte Prozesse bei der CGM zentral durch Automatismen geregelt. Dazu gehören:

- Verpflichtung aller Mitarbeiter auf Datengeheimnis nach DS-GVO sowie auf die Schweigepflicht nach §203 StGB (Verpflichtung sind als Anlagen in die Arbeitsverträge integriert, jeder neue Mitarbeiter wird somit vor dem Beginn der Tätigkeit verpflichtet)
- Schulung neuer Mitarbeiter auf Datenschutz zeitnah der Einstellung (Pflicht zur Schulung im Laufzettel)
- Datenschutz-Prüfung neuer Software/Module bereits während der Planungsphase (Integration im Planungsdokument)

## Kontrollprozesse

Die geltenden Regelungen werden laufend in jeder BU überwacht. Definierte Prozesse und Dokumentation zwingen alle Mitarbeiter zur Einhaltung dieser Regeln.

Darüber hinaus werden die Einhaltung dieser Regelungen und der geltenden Datenschutzgesetze durch regelmäßige Datenschutzaudits durch den DSB und Datenschutzkoordinatoren überprüft.

Ein DS-Audit und die Protokollierung erfolgen in standardisierter Form. Das Protokoll beinhaltet neben den Prüfergebnissen auch eine Risikoeinschätzung. Die Audits werden je BU und Standort jährlich durchgeführt. Die Protokolle werden unbegrenzt aufbewahrt.

Während des Audits werden sowohl die Gegebenheiten vor Ort als auch die Einhaltung der internen Regelungen der CGM überprüft. Im Bedarfsfall wird begleitend auch eine Fotodokumentation erstellt. Während der Prüfung werden die Verzeichnisse der Verarbeitungstätigkeiten auf Vollständigkeit und Aktualität überprüft.

Ergebnisse der Prüfung werden mit dem zuständigen Datenschutzkoordinator und dem General Manager der betroffenen BU besprochen. Zu jeder Überprüfung werden auf Basis der Empfehlungen des DSB Handlungsanweisungen abgeleitet. Zu jeder notwendigen Handlung werden Fristen und Verantwortliche für die Umsetzung vereinbart. Nach Ablauf dieser Frist wird die Durchführung der Handlung wiederholt kontrolliert.

Zusätzlich erfolgt eine Audit-Berichtserstattung an den Vorstand und zuständigen Senior Vice Presidents.

Vor der Einführung neuer Verfahren werden umfangreiche Einzelprüfungen des geplanten Verfahrens durchgeführt. Diese, teilweise zeitaufwändige Prüfungen werden durch Sofortmaßnahmen begleitet. In der Regel ist damit die Prüfung mit der Ausgestaltung des Verfahrens verbunden.

## Auftragskontrolle

Um die rechtskonforme Durchführung der Aufträge zu gewährleisten wurde die Vorgehensweise durch mehrere, für alle Mitarbeiter verpflichtende, detaillierte Verfahrens- und Fachanweisungen geregelt. Die Einhaltung der Regelungen wird von den Datenschutzkoordinatoren und von dem Datenschutzbeauftragten regelmäßig überprüft.

### Auftragskontrolle Fernwartung

Den Kunden wird grundsätzlich empfohlen, die Fernwartungs-Zugänge geschlossen zu halten und nur bei Bedarf und nach telefonischer Anfrage den Zugang frei zu schalten. Dieses Vorgehen liegt im Ermessen des Kunden.

Beim Zugriff auf Kundensysteme ausgehend von mobilen Arbeitsplätzen oder von Home-Offices, ist es verboten gleichzeitig Verbindung zu unsicheren, unbekanntem Netzwerken aufgebaut zu haben. Die Verbindung zu Kunden darf immer erst nach dem erfolgreichen Aufbau des Zugriffs zur Zentrale durch den VPN Client erstellt werden. Der VPN Client lässt in der standardmäßigen Einstellung keine weiteren Verbindungen zu. Diese Einstellungen dürfen nicht geändert oder kompromittiert werden.

Besondere Tätigkeiten, welche das Produkktivsystem verändern und/oder ein Risiko oder eine hohe Auswirkung auf die Prozesse beim Kunden haben, werden durch das 4-Augenprinzip über eine qualifizierte Person abgesichert.

Die darunterfallenden Tätigkeiten sind von dem jeweiligen Senior Service Manager definiert.

In der Regel werden Fernwartungs-Werkzeuge verwendet, bei welchen der Kunde aktiv den Zugang freigeben muss und die Aktivitäten mitverfolgen kann (z.B. Netviewer). Wenn die eingesetzte Fernwartungssoftware diese aktive Freigabe nicht voraussetzt, wird der Kunde über die Notwendigkeit des Zugriffs informiert und seine Zustimmung dafür angefordert. Diese Zustimmung (wer und wann) wird schriftlich dokumentiert.

Die Dokumentation des Fernwartungszugriffs und dessen Inhalt erfolgt immer in einem CRM-System. Es ist nicht erlaubt, undokumentierte Fernwartungszugriffe durchzuführen. Sämtliche Aktivitäten auf dem Kundensystem sind nachvollziehbar für Dritte sachlich beschrieben.

Hierbei wird immer:

- der ausführenden Mitarbeiter
- der Zeitpunkt (Datum/Uhrzeit) und die Dauer
- das Zielsystem (Test oder Produktiv bzw. Rechnername oder IP-Adresse)
- das Fernwartungsmedium (z.B. Netviewer, Remotedesktop, usw.)
- die Tätigkeit sachlich in Kurzform insbesondere, wenn Prozesse gestoppt/gestartet, Änderungen in Datenbanken, Änderungen in Konfigurationstabellen, Uploads und Downloads durchgeführt wurden
- der/die bei kritischen Tätigkeiten als 4-Augenprinzip herangezogene Kollegen

dokumentiert.

Die Aufzeichnung der durchgeführten Sitzungen, falls die Fernwartungssoftware diese Funktion unterstützt, wird nicht durchgeführt. Falls in bestimmten Situationen diese Aufzeichnung notwendig wäre, muss sie vom Kunden selbst und nur auf seinem System durchgeführt werden.

Ein Sonderfall stellt die Aufzeichnung eines Vorgangs dar, wo ausschließlich mit anonymisierten Testdaten gearbeitet wird. In diesem Falle wird nicht mit personenbezogenen Daten gearbeitet, die Aufzeichnung darf stattfinden.

Mit Kunden, die per Fernwartung betreut werden, müssen einmalig schriftliche

Datenschutzvereinbarungen, sog. AV Verträge (AVV), abgeschlossen werden. Diese Vereinbarungen regeln die Fernwartungszugriffe sowie Datenverarbeitung auf den Kundensystemen.

### Auftragskontrolle Datenimport

Für den Import von Kundendaten gilt ein generelles Verbot mit Erlaubnisvorbehalt. Der Import der Kundendaten ist somit nur in Ausnahmefällen, nur im Auftrag des Kunden und nur unter bestimmten Voraussetzungen erlaubt:

- es besteht keine andere Möglichkeit als nur mit Echtdateien des Kunden ein Problem zu beheben oder einen Kundenauftrag zu erfüllen
- Jeder Mitarbeiter muss vor dem Import personenbezogener Kundendaten seinen Vorgesetzten über den Vorgang informieren und dessen Genehmigung dafür einholen.
- Vor dem Import wird eine schriftliche Vereinbarung mit dem Kunden getroffen. Dies erfolgt ausschließlich in Form eines befristeten AV Vertrages. In dem Vertrag werden immer:
  - Zweck des Imports
  - Art und Umfang der Daten
  - Zeitraum der Nutzung
  - Löschfristen

eingeeben. Andere Formen der Vereinbarung sind nicht erlaubt.

Die Übermittlung der Daten erfolgt nur in der verschlüsselten Form.

Die Kundendaten werden nur auf den dafür vorgesehenen geschützten Serverbereichen importiert. Die Datenhaltung von nicht anonymisierten Kundendaten auf Arbeitsplatzrechner, Notebooks oder externen portablen Speichermedien ist strengstens untersagt.

Während des Analysevorgangs wird der Original-Datenträger des Kunden in einem Safe aufbewahrt. Alle Datenträger mit Kundendaten sind für die Aufbewahrung explizit als solche gekennzeichnet und erkennbar.

Jeder am Analyseprozess beteiligte Mitarbeiter dokumentiert seine Tätigkeiten und Abläufe mit den Kundendaten im CRM-System an dem initialen Eintrag, und ohne Personenbezüge.

Der Vorgang im CRM-System wird so lange "offen" gehalten, bis die Daten vernichtet oder an den Kunden zurückgesandt worden sind.

Am Ende des Vorgangs werden alle Datenbestände gelöscht. Für die Einhaltung der mit den Kunden vereinbarten Löschfristen ist der jeweilige Vorgesetzte der für den Import verantwortlichen Person zuständig.

Die Originaldatenträger werden entsprechend der getroffenen Vereinbarung vernichtet oder zurückgeschickt.

### Sicherheitsbuch Datenimporte

Neben der Dokumentation der durchgeführten Tätigkeiten in einem CRM-System werden bei jedem Datenimport bestimmte Angaben in einem speziell für diesen Zweck geführten Sicherheitsbuch eingetragen. Das Sicherheitsbuch wird in Papierform geführt und muss festgebundene Form haben.

In jedem Fachbereich ist dafür ein Verantwortlicher und ein Vertreter genannt, die die Einträge auf Richtigkeit und Vollständigkeit kontrollieren sowie die Übereinstimmung mit den abgeschlossenen AV Verträgen überprüfen.

Folgende Angaben werden zu jedem Import in dem Buch eingetragen:

- Kunde: Name, Kundennummer, Ort, Ansprechpartner
- Grund des Imports
- Genehmiger intern: Name, Funktion
- Bearbeiter: Name
- AV Vertrag (befristet): Datum des Abschlusses
- Eingang: Datum, Empfänger
- Kopie auf Server: Servername, Verzeichnis
- Aufbewahrungsort des Originaldatenträgers (nur falls Import mittels Datenträger)
- Bearbeitung Beginn: Datum
- Bearbeitung Ende: Datum
- Löschung der Kopie vom Server: Datum, Name Mitarbeiter
- Originaldaten nach Abschluss der Arbeiten: Datenträger vernichtet oder zurückgeschickt, Datum, Name Mitarbeiter, Art der Vernichtung

## Incident Response Management

Die zentrale IT-Abteilung (CGM GroupIT) stellt sicher, dass angemessen auf jegliche aktuellen oder zu erwartenden Vorfälle bezüglich der internen oder in der Obhut befindlicher Informationssysteme reagiert werden kann.

Es gelten hierzu die folgenden allgemeinen Richtlinien:

- Datacenter Security Incident Management
- Datacenter Incident Management
- DataCenter Koblenz floor plan for emergency teams
- Incident Management
- Security Incident Management Policy
- IT Notfallplan Standort Koblenz

Mit den in den Richtlinien beschriebenen Maßnahmen soll sichergestellt werden, dass:

- Sicherheitsvorfälle frühzeitig erkannt und deren Auswirkung minimiert oder begrenzt werden können
- Sicherheitsvorfälle einheitlich zentralisiert gemeldet werden
- Bei Eintreten eines Vorfalls strukturierte und zeitsparende Vorgehensmodelle in Verbindung mit klaren Verantwortlichkeiten existieren wie z. B. Erste Maßnahmen, Vorgehensweisen bei Notfällen u. Ausfällen, Reihenfolge der Alarmierung der Verantwortlichen, Wiederanlaufverfahren, hierarchische aufgebaute Eskalationsketten innerhalb der Organisations-Hierarchie.
- Vorfälle nachvollziehbar dokumentiert, begutachtet u. analysiert werden können.
- Die Wiederholung des Vorfalls durch Ergreifen nachhaltiger Maßnahmen vermieden werden kann

## Privacy by Default



Es gibt ein einheitliches Konzept zu Datenschutz-freundlichen Voreinstellungen und Standards innerhalb der IT basierend auf der internen Richtlinie CGM Information Security Policy. Hierunter fallen

- Voreinstellungen des Betriebssystems für Client PCs u. der automatischen Bereitstellung und Verteilung von Software-Applikationen.
- Voreinstellungen des Betriebssystems für aus Vorlagen bereitgestellten virtuellen Servern.
- automatische Festplattenverschlüsselung für Client Endgeräte (Notebooks, PCs und Mobiltelefone)
- Limitierung der erhobenen Log- und Monitoring-Daten auf den zur Ermittlung von gesetzlich relevanten Maßnahmen notwendigen Umfang. Hierzu gibt es eine allgemeingültige Definition in der Richtlinie Monitoring- und Log-Policy.

## Zertifizierungen Rechenzentrum in Koblenz

Rechenzentrum Koblenz:

- TÜV InterCERT Category 3 - highly available Data Center with 24/7 operation - sustainability (according to procedure TIC-PR-PC-08-Annex 7) Certificate no. 12-T-0000300-TIC
- Management system as per ISO/IEC 27001:2013, Certificate Registration No. TAD ISMS 19907, scope "All CGM OneGroup and hosting services provided by CGM GroupIT", Valid Statement of Applicability (SoA): v11, 03.05.2019
- Fortidata Agreement als zugelassener Hostingprovider für CGM Frankreich (<https://esante.gouv.fr/node/2361>)

## Zertifizierungen Rechenzentrum in Frankfurt

Rechenzentrum Frankfurt (FRA6 u. FRA8), betrieben von interxion:

- INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013, Certificate No: IS 537141, scope "The delivery of data centre services, as defined by management and in accordance with the Statement of Applicability version 4 dated 10 July 2015
- Management system as per ISO/IEC 27001:2013, Certificate Registration No. TAD ISMS 19907, scope "All CGM OneGroup and hosting services provided by CGM GroupIT", Valid Statement of Applicability (SoA): v11, 03.05.2019
- Fortidata Agreement als zugelassener Hostingprovider für CGM Frankreich (<https://esante.gouv.fr/node/2361>)



## Beiblatt 1: Datenverarbeitung durch THERAFOX

---

Für die Datenverarbeitung durch das Produkt THERAFOX gelten die folgenden Besonderheiten. THERAFOX ist als Variante THERAFOX PRO speziell für medizinisches Fachpersonal erhältlich. Wo notwendig wird im Folgenden speziell auf THERAFOX PRO eingegangen. Bei Nennung von THERAFOX gelten die Beschreibungen auch für die Variante THERAFOX PRO.

### Authentifizierung der aufrufenden Software

THERAFOX wird als separate Software als Auftragsverarbeitung in andere Software integriert, z.B. ein Arztinformationssystem (AIS) bzw. Praxisverwaltungssystem (PVS). Über diese Software wird THERAFOX aufgerufen. Der Hersteller dieser aufrufenden Software erhält von der ifap Credentials (Nutzername, Passwort) für seine Software. Die Credentials werden auf einem separaten Weg zum Hersteller transportiert. Sie werden als geschütztes PDF an den Hersteller per E-Mail versendet. Das Passwort für das geschützte Dokument wird per SMS, Fax oder über ein Telefonat mitgeteilt. Im Falle der Übermittlung per Fax ist der Hersteller zuvor telefonisch zu benachrichtigen und die Faxnummer erneut zu verifizieren. In jedem Fall muss in der Folge eine Überprüfung stattfinden, ob der Hersteller das Passwort und seine Zugangsdaten richtig erhalten hat.

Die Credentials werden bei der ifap in einer KeyPass-Datenbank gespeichert. Der Zugang zur KeyPass Datenbank ist ifap-intern auf den Personenkreis beschränkt, der für die Leistungserbringung gegenüber den Herstellern Zugriff auf die Daten benötigt.

Diese Credentials werden von der aufrufenden Software verwendet, um sich beim THERAFOX PRO Service zu authentifizieren. Dies erfolgt über https Basic Auth und die Credentials sind BASE64 kodiert. Die aufrufende Software erhält ein Sicherheits-Token zurück (OAuth2). Nach der Authentifizierung ist die aufrufende Software über das Token dazu autorisiert, Anfragen an THERAFOX zu senden. Das Token wird nach einer Stunde ungültig. Der Authentifizierungsprozess erfolgt bei jeder Nutzung von THERAFOX. Sind die Credentials nicht in der aufrufenden Software hinterlegt, ist eine Nutzung von THERAFOX nicht möglich.

### Einsatz von THERAFOX PRO im Wege der Auftragsverarbeitung bei

Die Datenübertragung an THERAFOX als Auftragsverarbeitung (z.B. in Arztpraxen) setzt einen unterschriebenen Auftragsverarbeitungs-Vertrag (AV-Vertrag) voraus. Über eine Prüfung der Kennnummern des Auftraggebers (BSNR oder Kundennummer) wird sichergestellt, dass in diesen Konstellationen THERAFOX nicht ohne Abschluss eines solchen AV-Vertrags genutzt werden kann. Die Freischaltung erfolgt durch die ifap nur bei vorliegendem AV-Vertrag in einer separaten Software, auf die nur die ifap-Mitarbeiter Zugriff haben, die für die Freischaltung verantwortlich sind. Die Daten werden in der separaten Software in einer verschlüsselten Datenbank abgelegt. Der Zugriff für ifap-Mitarbeiter zur Eintragung der Informationen zur Freischaltung ist personalisiert und wird über Nutzername und Passwort eingeschränkt.

## Verschlüsselung der Kommunikation

Alle Kommunikation zwischen der aufrufenden Anwendung und THERAFOX PRO erfolgt verschlüsselt über das HTTP-Protokoll mit Verschlüsselung per Transport Layer Security (TLS 1.2 bei Implementierung mit Perfect Forward Secrecy oder TLS 1.3+).

## Speicherung von Daten zur Nachvollziehbarkeit von Vorkommnissen

Um im Falle der Meldung eines möglichen Vorkommnisses zum Medizinprodukt den Vorgang der Anfrage und Ergebnisübermittlung zu rekonstruieren, werden von THERAFOX Daten gespeichert. Dies ist medizinproduktrechtlich zwingend. Die komplette Anfrage und die komplette strukturierte Antwort werden als JSON-Objekte in einer Datei gespeichert. Der Datenträger, auf dem die Datenspeicherung erfolgt, ist nach dem Advanced Encryption Standard verschlüsselt (AES-256). Für den Zugriff auf den Datenträger besteht ein Benutzerrechtekonzept. Der Zugriff auf den Datenträger ist nur einem sehr eingeschränkten Kreis von Systemadministratoren möglich, um Installations-, Konfigurations- und Wartungsarbeiten durchzuführen, und um im Falle einer Meldung auf die gespeicherten Daten zur Nachvollziehbarkeit von Vorkommnissen zuzugreifen.

Die Daten werden dazu bei Nutzung des ifap praxisCENTER 3 wie folgt beschrieben pseudonymisiert: Bei einer Anfrage nach Check-Ergebnissen an THERAFOX PRO werden die Anfrageinhalte und das Ergebnis mit einer kodierten Anfrage-ID versehen. Diese Anfrage-ID ist pseudonymisiert. Sie besteht aus folgenden Komponenten:

- Patientenummer aus dem AIS bzw. PVS
- BSNR (bzw., falls nicht vorhanden, Kundennummer)
- Secret

Diese Komponenten werden zur Bildung der kodierten Anfrage-ID lokal in der Software beim Kunden vor Übermittlung an die Cloud in eine kodierte Zeichenfolge umgewandelt (Hashing). Dabei kommt das SHA-2-256-Verfahren zum Einsatz. Anstelle der Patientenummer und BSNR/Kundennummer wird mit der Anfrage nur diese kodierte Anfrage-ID an THERAFOX PRO übermittelt. Eine Rückverfolgbarkeit zu Patientenummer und BSNR/Kundennummer ausgehend von der Anfrage-ID ist nicht möglich. Nur, wenn der Auftraggeber etwa bei einem Vorkommnis Patientenummer und BSNR/Kundennummer mitteilt, kann die ifap die zugehörige Anfrage-ID ermitteln.

## Ort der Datenverarbeitung

Die hier beschriebenen Datenverarbeitungstätigkeiten zum Produkt THERAFOX werden in den Rechenzentren Koblenz (betrieben von der CGM SE) und Frankfurt am Main (betrieben von interxion) durchgeführt.