# Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen

**Susanne Edens**

**Friedrich- Naumann- Str. 10**

**44359 Dortmund**

- Verantwortlicher -

nachstehend Auftraggeber genannt

und

**CompuGroup Medical Deutschland AG**

**Maria Trost 21**

**56070 Koblenz**

- Auftragsverarbeiter -

nachstehend Auftragnehmer genannt

## 1. Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Aufbau und Durchführung einer Videositzung mittels CGM ELVI oder CLICKDOC Videosprechstunde (nachfolgend nur CGM Videosprechstunde genannt)
- Abwicklung von allgemeinen oder Supportanfragen, Registrierungen und Vertragsabschlüssen in Bezug auf die CGM Videosprechstunde

Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sind im Hauptvertrag zu vereinbaren.

## 2. Dauer des Auftrags

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monaten zum Jahresende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## 3. Konkretisierung des Auftragsinhalts

**(1) Art und Zweck der vorgesehenen Verarbeitung von Daten**

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Aufbau einer Videositzung mittels der CGM Videosprechstunde. Zum Aufbau der Videositzung mittels der CGM Videosprechstunde wird die IP-Adresse des Auftraggebers und die seiner Gesprächspartner an den Server der La-Well Systems GmbH übermittelt. Die übermittelten IP-Adressen werden nicht persistent gespeichert.
- Durchführung einer Videositzung zwischen Auftraggeber und Gast mit Zugangscode: Der Name und Zugangscode des Gastes, mit dem der Auftraggeber eine CGM Videosprechstunde durchführt, werden an den Server der La-Well Systems GmbH übermittelt. Name und Zugangscode werden gespeichert, bis der Kunde diese Angaben in seinem CGM Videosprechstunden -Profil löscht.
- Optional: Bei Nutzung des Whiteboards innerhalb der CGM Videosprechstunde werden die hochgeladenen Dateien temporär und verschlüsselt auf dem Server der La-Well Systems GmbH gespeichert. Nach Ablauf der Videositzung werden die Dateien gelöscht.

  Die La-Well Systems GmbH weist ausdrücklich darauf hin, dass das Whiteboard nicht zur Befundung bestimmt ist. Trotzdem kann durch technisch-organisatorischen Maßnahmen nicht ausgeschlossen werden, dass Kunden oder deren Gäste über das Whiteboard besondere Kategorien personenbezogener Daten austauschen. Bei der Verwendung entgegen der Zweckbestimmung ist der Nutzer verpflichtet, die gesetzlichen Bestimmungen zu beachten und umzusetzen.
- Optional: Bei Nutzung des Chats und des Desktop-Sharings innerhalb der CGM Videosprechstunde kann durch technisch-organisatorischen Maßnahmen nicht ausgeschlossen werden, dass Kunden oder deren Gäste besondere Kategorien personenbezogener Daten übertragen. Der Inhalt des Chats und des Desktop-Sharings wird peer-to-peer übertragen und nicht gespeichert.

- Zur Abwicklung von allgemeinen oder Supportanfragen, Registrierungen und Vertragsabschlüssen in Bezug auf die CGM Videosprechstunde werden personenbezogene Daten (Vertrags-, Kontakt- und Registrierungsdaten) an die Compu Group Medical SE und / oder weitere konzerninterne Unternehmen weitergeleitet.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

**(2) Art der Daten**

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

☒ IP-Adresse (wird von unserem DDoS-Mitigations Dienstleister Cloudflare bis zu einem Jahr gespeichert)

☒ Name und Zugangscode des Gastes (Speicherung erfolgt bis der Nutzer die Daten löscht, bzw. seinen Vertrag kündigt)

☒ Optional bei Versand des Zugangscodes an den Gast: E-Mail-Adresse oder Handynummer des Gastes (anonymisierte Speicherung für 3 Monate)

☒ In Abhängigkeit von den Inhalten, die durch den Kunden durch den Chat oder das Desktop-Sharings ausgetauscht werden: Besondere Kategorien personenbezogener Daten (Gesundheits- oder Sozialdaten) (ohne Speicherung)

☒ In Abhängigkeit von den Inhalten, die durch den Kunden und seine Gäste bei der Nutzung des Whiteboards ausgetauscht werden: Besondere Kategorien personenbezogener Daten (Gesundheits- oder Sozialdaten) (Verschlüsselte Speicherung für die Dauer der Videositzung)

☒ Vertrags-, Kontakt- und Registrierungsdaten (Wir verpflichten uns gemäß Datenschutzgesetz, sämtliche Vertragsdaten, sämtliche Protokolldaten und sämtliche Daten zum technischen Betrieb nach Kündigung eines 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 eines Vertrages gelöscht.

☒ Video- und Sprachaufnahmen (ohne Speicherung)

☒ Gesundheitsdaten im Rahmen der Video- und Sprachaufnahmen (ohne Speicherung)

**(3) Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Angehörige eines Gesundheits- oder Sozialberufes und deren Mitarbeiter

☒ Patienten/Gäste des Kunden

## 4. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

## 5. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Hans Gerlitz, CompuGroup Medical SE, Tel.: 0261 8000 1667, E-Mail: hansjosef.gerlitz@cgm.com bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten

ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
Bei der Durchführung der Arbeiten die Gesundheitsdaten betreffen setzt der Auftragnehmer nur Beschäftigte ein, die auf die ärztliche Schweigepflicht gemäß §203 StGB belehrt und verpflichtet wurden.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

| Firma Unterauftragnehmer | Anschrift/Land | Leistung |
|---|---|---|
| Interxion Deutschland GmbH | Hanauer Landstraße 298<br>60314 Frankfurt am Main<br>Deutschland | Serverhosting und -management |
| CompuGroup Medical SE | Maria Trost 21<br>56070 Koblenz | Serverhosting und -management |

| | | |
|---|---|---|
| | Deutschland | |
| CompuGroup Medical SE und / oder weitere konzerninterne Unternehmen | Maria Trost 21<br>56070 Koblenz<br>Deutschland | Abwicklung von allgemeinen oder Supportanfragen, Registrierungen und Vertragsabschlüssen in Bezug auf die CGM Videosprechstunde |
| Message Networks GmbH | Stresemannstr. 12<br>40210 Düsseldorf | SMS-Dienstleister. Versendung von SMS aus der CGM Videosprechstunde. |

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## 9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 10. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## 12. Informationspflichten, Schriftformklausel

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

## 13. Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zusatzvereinbarung unwirksam oder undurchführbar sein oder nach Unterzeichnung unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

**Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit**

Zentrales Datenschutzmanagement CompuGroup Medical SE

Standort Bünde – La-Well Systems GmbH

# 1. Vertraulichkeit

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

## Zutrittskontrolle

### Sicherungsmaßnahmen des Gebäudes Standort Bünde

Folgende Sicherungsmaßnamen des Bürogebäudes bestehen:

### Sicherung und Zugang zum Bürogelände

Das Bürogebäude ist durch einen Zaun (2m Höhe) von der Straße getrennt. Das Tor zum Bürogelände ist nur zu Bürozeiten geöffnet. Nach Schließung des Büros ist kein Zutritt zum Bürogelände möglich.

Der Zutritt zu den Büroräumen der La-Well Systems GmbH ist nur Mitarbeitern gestattet und nur über das Schließsystem möglich.

Gäste werden von den Mitarbeitern am Eingang in Empfang genommen und dürfen sich nicht frei in den Büroräumen bewegen. Alle Gäste werden im zentralen Besucherbuch eingetragen.

### Schließsystem Gebäude- und Eingangstür/en

An allen Eingängen des Bürogebäudes ist der Zugang nur mit einem entsprechenden Schlüssel möglich. Der Zugang zur Büroetage ist nur mit einer passenden Schlüsselkarte möglich.

## Zugriffskontrolle zum 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 liegt ein Zugangs- und Zugangsrechtekonzept vor, durch das

gewährleistet wird, dass die Nutzungsberechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für CGM ELVI/CLICKDOC VIDEOSPRECHSTUNDE:

Personenbezogenen Daten von Kunden von CGM ELVI/CLICKDOC VIDEOSPRECHSTUNDE werden auf den Servern der La-Well Systems GmbH, FastBill GmbH, CGM SE und Interxion Deutschland GmbH in Deutschland gespeichert.

Der Zugang zu den Daten auf den Servern der La-Well Systems GmbH und der FastBill GmbH ist entsprechend dem Zugangs- und Zugangsrechtekonzept nur ausgewählten Mitarbeitern möglich, die diese für Ihre Tätigkeit benötigen.

Die Administration des Produktivservers, der Backups und des Monitorings obliegen den Dienstanbietern CGM SE und Interxion Deutschland GmbH und sind vertraglich bzw. in einem SLA festgehalten

### Systemadministration

Die Administration der Datenverarbeitungssysteme wird von internen Mitarbeitern der CGM SE und dem IT-Beauftragten der La-Well System GmbH durchgeführt.

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

Für CGM ELVI/CLICKDOC VIDEOSPRECHSTUNDE:

Die Administration des Produktivservers, der Backups und des Monitorings obliegen den Dienstanbietern CGM SE und Interxion Deutschland GmbH und sind vertraglich bzw. in einem SLA festgehalten

## 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.

Datenweitergabe und -transport beruhen auf einheitlichen Systemen zur Authentifizierung von Benutzern durch Benutzerkennung, 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.

Die Vernichtung von Datenträgern/Festplatten etc. erfolgt im Bedarfsfall über ein zertifiziertes Drittunternehmen.

Nicht mehr benötigte Dokumente in Papierform werden in den Bereichen vernichtet. Dokumente, die personenbezogene Daten beinhalten, in Aktenvernichtern mit Sicherheitsstufe 3 bzw. 4 im Sinne der DIN 66399. Die Entsorgung von größeren Mengen der Dokumente erfolgt im Bedarfsfall über ein zertifiziertes Drittunternehmen.

## 3. Verfügbarkeit und Belastbarkeit

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

### Verfügbarkeitskontrole Betriebsbereitschaft

Der Betrieb wird durch Personal vor Ort Montag bis Freitag von 8:00 Uhr bis 17:00 Uhr sichergestellt.

### Datensicherung Standort Bünde

- Es findet eine wöchentliche Sicherung der Daten statt.
- Jeder Sicherungsvorgang wird manuell überprüft.

### 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

# 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. Der Mutterkonzern der La-Well Systems GmbH 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 der La-Well Systems GmbH als 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.

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 Entscheidungen des Beauftragten für den Datenschutz zur Abhilfe der Datenschutzverletzung sind durch die jeweiligen Geschäftsführungen und Geschäftsbereichsleiter zu respektieren.

Der Datenschutzbeauftragte berichtet an den Vorstand der CGM und die General Manager der jeweiligen BU‘s. 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.

Zuwiderhandlungen, 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 (inkl. Fernwartung)
- 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 Tätigkeitverpflichtet)
- 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 wir die Durchführung der Handlung wiederholt kontrolliert.

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

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.

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 Produktivsystem 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. Anydesk). Wenn die eingesetzte Fernwartungssoftware diese aktive Freigabe nicht voraussetzt, wird der Kunde über die Notwendigkeit des Zugriffes informiert und seine Zustimmung dafür angefordert. Diese Zustimmung (wer und wann) wird schriftlich dokumentiert.

Die Dokumentation des Fernwartungszugriffes 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
- das Fernwartungsmedium (z.B. Anydesk, Teamviewer, 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

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.

## 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.

Für CGM ELVI/CLICKDOC VIDEOSPRECHSTUNDE:

Die initiale Einstellung im CGM ELVI/CLICKDOC VIDEOSPRECHSTUNDE - Account eines Nutzers sieht vor, dass dieser in der Kontaktsuche nicht sichtbar ist und damit nicht durch anderer CGM ELVI/CLICKDOC VIDEOSPRECHSTUNDE - Nutzer gefunden oder per Video angerufen werden kann.