CGM PROTECT
IT-Security in Healthcare

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

gemäß Art. 28 DSGVO

zwischen

Name Kunde / Einrichtung

Straße

PLZ / Ort

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: Betrieb (inkl. Hosting) von einem oder mehreren vertraglich vereinbarten Produkten aus dem CGM PROTECT Portfolio sowie Service und Support für diese Produkte. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sind im Hauptvertrag zu vereinbaren.

2. DAUER DES AUFTRAG

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

3. KONKRETISIERUNG DES AUFTRAGSINHALTS

3.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

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

Produkt	Produktbezeichnung	Art und Zweck der Aufgaben des Auftragnehmers
CGM ENDPOINT 360°	CGM ENDPOINT 360° ist eine Kombination aus einer Endpoint-Protection-Plattform (EPP), die eine traditionelle Antivirensoftware enthält, und zusätzlich einen State-of-the-Art-Endpoint-Schutz mit einem cloudbasierten Endpoint-Detection-and-Response-Dienst (EDR) kombiniert.	Betrieb (inkl. Hosting), Service und Support des Produktes
CGM FIREWALL	Bei der CGM FIREWALL handelt es sich um eine Firewall-Lösung zum Schutz des gesamten Netzwerks des Auftraggebers vor Bedrohungen von außerhalb und wird daher dem lokalen Netzwerk physisch vorgeschaltet.	Betrieb (inkl. Hosting), Service und Support des Produktes
CGM SECURE WIFI	CGM SECURE WIFI stellt über ein oder mehrere hardwarebasierte Access Points einen sicheren WLAN-Zugang zum angeschlossenen Netzwerk des Auftraggebers oder in einem abgetrennten Netzbereich für Patienten zur Verfügung.	Betrieb (inkl. Hosting), Service und Support des Produktes
CGM MOBILE WORK	CGM MOBILE WORK verbindet zwei oder mehrere Endgeräte miteinander, welche sich an unterschiedlichen Standorten befinden.	Betrieb (inkl. Hosting), Service und Support des Produktes

3.2 CGM PROTECT Allgemein

3.2.1 Art der Daten

Personenbezogene Daten des Auftraggebers und des Servicepartners wie folgt:

– Kunde:

- Anrede, Vor- und Nachname des Inhabers
- Bezeichnung der Einrichtung
- postalische Anschrift
- E-Mail-Adresse
- SAP Kunden-ID

Die Erbringung der vertraglich vereinbarten Datenverarbeitung außerhalb der Europäischen Union und außerhalb der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

CompuGroup Medical

3.3 CGM ENDPOINT 360°

3.3.1 Art der Daten

Personenbezogene Daten des Servicepartners wie folgt:

- E-Mail-Adresse

3.3.2 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Auftraggeber
- Mitarbeiter des Auftraggebers
- Mitarbeiter des Servicepartners

3.4 CGM FIREWALL

3.4.1 Art der Daten

Personenbezogene Daten des Auftraggebers und des Servicepartners wie folgt:

– Kunde:

- Konfigurationsdaten der Firewalls
- Seriennummer und IP-Adresse der Firewalls
- Trafficdaten aus dem Netzwerk der Einrichtung

– Servicepartner:

- Anrede, Vor- und Nachname der Mitarbeiter

3.4.2 Kategorien betroffener Personen Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Auftraggeber
- Mitarbeiter des Auftraggebers
- Mitarbeiter des Servicepartners

3.5 CGM SECURE WIFI

3.5.1 Art der Daten

Personenbezogene Daten des Auftraggebers und des Servicepartners wie folgt:

– Kunde:

- Konfigurationsdaten der Access Points
- Seriennummer und IP-Adresse der Access Points
- Trafficdaten aus dem Netzwerk der Einrichtung

– Servicepartner:

- Anrede, Vor- und Nachname der Mitarbeiter

3.5.2 Kategorien betroffener Personen. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Auftraggeber
- Mitarbeiter des Auftraggebers
- Mitarbeiter des Servicepartners

3.6 CGM MOBILE WORK

3.6.1 Art der Daten

Personenbezogene Daten des Auftraggebers und des Servicepartners wie folgt:

– Kunde:

- Daten zur Verwaltung der Verbindung:
  - SAP Kunden-ID
  - Anmelde-ID
- Daten zur Laufzeit einer Verbindung:
  - IP-Adresse (Praxis und Heimarbeitsplatz)
  - SAP Kunden-ID
  - Streaming-Daten (Bildübertragung):
    Es wird über eine Verbindung die Änderungen des Bildschirminhalts des Servers (Remotestation) als Bildpunkt übertragen. Die Darstellung des Bildschirmes kann nur auf dem Client angezeigt werden. Maus- und Keyboardeingaben werden zur Verbindungszeit über einen Rückkanal auf den Server (Remotestation) übertragen. Wird die Verbindung unterbrochen, so sind keinerlei Informationen auf einem Server des Auftragsnehmers zwischengespeichert.

3.6.2 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Auftraggeber
- Mitarbeiter des Auftraggebers

4. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

4.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen[1] 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.

4.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [Einzelheiten siehe TOMs[1]].

4.3 Die technischen und organisatorischen Maßnahmen[1] 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.

[1] Die produktspezifischen technischen und organisatorischen Maßnahmen (TOMs) des Auftragnehmers finden Sie unter: cgm.com/ti-download

5. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

5.1 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.

5.2 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 DSGVO; 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 DSGVO. 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.

c) 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.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten siehe TOMs[1]].

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) 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.

g) 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.

h) 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.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

7. UNTERAUFTRAGSVERHÄLTNISSE

7.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.2 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 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
CGM ENDPOINT 360°		
PAV Germany GmbH Deutschland	Dr.-Alfred-Herrhausen Allee 26 47228 Duisburg	3rd Level Support für die genannten Produkte, Untersuchung von Dateien auf Schadsoftware
Microsoft Corporation (Azure), Irland	One Microsoft Way Redmond, WA 98052-6399 USA	Betrieb (inkl. Hosting), der genannten Produkte auf Servern in der EU im Auftrag der PAV Germany GmbH
Ihr autorisierter Vertriebs- und Service-Partner	Zuordnung gemäß PLZ-Zugehörigkeit[2] in Deutschland	Fernwartung und Service-Arbeiten vor Ort
CGM FIREWALL und CGM SECURE WIFI		
ADN – Advanced Digital Network Distribution GmbH	Josef-Haumann-Straße 10 44866 Bochum	Beschaffung und Logistik
CGM IT Solutions und Services GmbH	Maria Trost 25, 56070 Koblenz	Beschaffung und Logistik
WatchGuard Technologies Inc.	505 Fifth Avenue South Suite 500 Seattle, WA 98104 USA	Bereitstellung der WatchGuard-Cloud, 3rd Level Support des Produktes
Amazon Web Services, Inc.	Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA	Hosting, Diagnose und Betrieb der WatchGuard Cloud im Auftrag der WatchGuard Technologies Inc. an Standorten in der EU
Ihr autorisierter Vertriebs- und Service-Partner	Zuordnung gemäß PLZ-Zugehörigkeit[2] in Deutschland	Fernwartung und Service-Arbeiten vor Ort
CGM MOBILE WORK		CGM MOBILE WORK
Team2Work GmbH	Hildastr. 16 76571 Gaggenau	L3 Support für CGM
Ihr autorisierter Vertriebs- und Service-Partner	Zuordnung gemäß PLZ-Zugehörigkeit[2] in Deutschland	Fernwartung und Service-Arbeiten vor Ort

[2] Die aktuelle Liste von autorisierten Vertriebs - und Service Partnern finden Sie unter: cgm.com/cgm-protect-dsgvo

Weitere Unterauftragnehmer, die von WatchGuard Technologies, Inc. eingesetzt werden:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
WatchGuard Cloud		
Mailgun Technologies, Inc.	E-Mail sending service for WatchGuard Cloud. Receives email addresses and email bodies from WatchGuard Cloud then manages the sending of them to recipients as specified in the WatchGuard Cloud user interface.	US or EU based on WatchGuard Cloud Region
Firebox		
Proofpoint, Inc.	Anti-spam service for Fireboxes (spamBlocker).	United States
Forcepoint, LLC	Cloud-based URL categorization (WebBlocker). The Firebox's IP address is visible to Forcepoint as the sender of the URL to be categorized.	United States, Ireland

Die Auslagerung auf Unterauftragnehmer und / oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

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

7.4 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.

7.5 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers; diese kann auch als allgemeine Genehmigung gem. Art. 28 Abs. 2 Satz 2 DSGVO erteilt werden; sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. KONTROLLRECHTE DES AUFTRAGGEBERS

8.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.

8.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

8.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

9. MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

9.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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.

9.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

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

10.2 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

11.1 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.

11.2 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.

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

12. INFORMATIONSPFLICHTEN, SCHRIFTFORMKLAUSEL

12.1 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.

12.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen oder elektronischen 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.

STAND: DEZEMBER 2025

CompuGroup Medical

CGMCOM-29029_CONPRO_1225_MDI