

CGM MEDICAL IAAS

vmw Leistungsbeschreibung

Inhaltsverzeichnis

1 Produktbeschreibung	1
2 Leistungselemente	2
3 Szenarien mit Notwendigkeit eine Backup-Rücksicherung	3
4 Zusatzoptionen	4
5 Voraussetzungen und Mitwirkungspflichten	4
6 Lizenzierung	4
7 Service Paket	5
8 SLA	5
9 Sonstige Bestimmungen	6

1 Produktbeschreibung

Mit **CGM Medical IaaS vmw** bieten wir unseren Kunden die Möglichkeit, Serverfunktionalitäten in ein Rechenzentrum zu verlagern, **als Infrastructure-as-a-Service (IaaS)**. Kunden erhalten dabei eine **maßgeschneiderte virtuelle Serverlösung**, ohne hohe Einmalzahlungen leisten zu müssen. Die bereitgestellte Infrastruktur ist **flexibel skalierbar** und kann an veränderte Anforderungen angepasst werden.

Unsere Lösung basiert auf einer hochverfügbaren Infrastruktur mit virtuellen Maschinen (**VMs**) in einem **C5-zertifizierten Rechenzentrum** in Deutschland.

Wichtig: Das CGM Medical IaaS vmw wird als „Self-Service“ angeboten. Das bedeutet, dass der Kunde die Verantwortung für den Inhalt der bereitgestellten VM trägt und eigenständig Dienstleistungen seiner Wahl beauftragen kann, um spezifische Aufgaben zu erfüllen. Mit CGM Medical IaaS vmw stellt die CompuGroup Medical Deutschland AG (**CGM**) eine **VMware-basierte Rechenzentrumsinfrastruktur** zur Verfügung. Kunden wie niedergelassene Ärzte oder **medizinische Versorgungszentren (MVZ)** erhalten über **VPN gesicherten Zugriff** auf eine praxiseigene, skalierbare und hochverfügbare IT-Infrastruktur. Das Design der IaaS-Umgebung ist speziell auf den hohen Schutzbedarf sensibler medizinischer Daten ausgerichtet und garantiert eine datenschutzkonforme Speicherung in einem C5-zertifizierten Rechenzentrum in Deutschland.

Die Verwaltung, Lagerung und Wartung der Infrastruktur-Hardware

liegt vollständig im Verantwortungsbereich der CGM und ihrer Subunternehmer.

Hinweis: Auf Wunsch stellen wir dem Kunden entgeltlich Detailunterlagen zur **C5:2020-Zertifizierung** zur Verfügung, ausgestellt durch eine unabhängige Wirtschaftsprüfungsgesellschaft.

Weitere Vorteile einer „CGM Medical IaaS vmw“ Umgebung:

- **Nutzungsbezogene Abrechnung:** Ressourcen wie z. B. Lizenzen werden verbrauchsabhängig abgerechnet, wodurch Kosten flexibel und transparent gestaltet werden können.
- **Physische Sicherheit:** Umfassende Sicherheitsmaßnahmen wie Zutrittskontrollen im Rechenzentrum, Schutz vor Diebstahl, Feuer und Wasserschäden, klimatisierte Serverräume, redundante Stromversorgung sowie mehrfach redundante Breitbandinternetzugänge gewährleisten höchste Betriebssicherheit.
- **Erweiterte Datensicherung:** Die Datensicherungsumgebung ist in einem separaten Brandabschnitt untergebracht. Optional können Sicherungskopien (Backup Copy) auch außerhalb des Rechenzentrums gespeichert werden.
- **Einfache Standortvernetzung:** Die Umgebung ermöglicht eine unkomplizierte Vernetzung weiterer Praxisstandorte, wie beispielsweise Niederlassungen, und unterstützt so die Expansion von Praxen.
- **Planungssichere Kosten:** Durch eine standardisierte Infrastruktur können Kosten langfristig kalkuliert und unerwartete Ausgaben vermieden werden.

CGM MEDICAL IAAS

vmw Leistungsbeschreibung

- **Kosteneffizienz:** Im Vergleich zu On-Premise-Lösungen vor Ort bietet die IaaS-Umgebung deutliche Kostenvorteile.
- **Keine Hardwaremodernisierung:** Regelmäßige Investitionen in neue Hardware entfallen, da die Infrastruktur durch die CGM kontinuierlich auf dem neuesten Stand gehalten wird.

2 Leistungselemente

Firewall

Für einen optimalen Betrieb und die Einhaltung der KBV-IT Sicherheitsrichtlinie (Quelle: <https://hub.kbv.de/display/itsrl>) wird eine zusätzliche UTM-Firewall-VM mit erweiterten Sicherheitsfunktionen und zentralem Management bereitgestellt. Diese Firewall ist ein integraler Bestandteil der CGM Medical IaaS vmw Lösung und gewährleistet höchste Sicherheitsstandards.

Ein weiterer Vorteil dieser Firewall ist die Einrichtung der BoVPN-Verbindung (Branch Office VPN), die eine sichere Anbindung an das lokale Praxisnetzwerk ermöglicht.

Empfehlung: Für die Konfiguration der VPN-Strecken wird dringend empfohlen, an den Praxisstandorten eine feste öffentliche IP-Adresse durch den Internet-Service-Provider (ISP) zu beantragen. Dies stellt eine stabile und zuverlässige Verbindung sicher.

VLAN

Zur Erhöhung der Sicherheit wird jedem gebuchten Paket ein eigenes VLAN innerhalb des Rechenzentrums zugewiesen. Dadurch erhält jeder Kunde ein privates Netzwerk, das eine vollständige Trennung von anderen Netzwerken sicherstellt.

Die Definition des internen IP-Netzwerks erfolgt individuell durch den Kunden, sodass spezifische Anforderungen und bestehende Netzwerkkonfigurationen berücksichtigt werden können.

Öffentliche IP

Jedes IaaS-Paket beinhaltet standardmäßig eine öffentliche IP-Adresse. Auf Wunsch können zusätzliche öffentliche IP-Adressen gegen eine Gebühr hinzugebucht werden, um spezifische Anforderungen zu erfüllen.

Virtueller Server / Virtuelle Maschinen

Auf Basis der skalierbaren VMWARE Virtualisierungstechnologie werden dem Kunden virtuelle Server (auch bezeichnet als VM = Virtuelle Maschinen) zur Verfügung gestellt.

Die Systemadministration des Kunden beginnt nach der Installation und ab Übergabe der Zugangsdaten durch die CGM an den Kunden. Je nach Kundenanforderung können auf den virtuellen Servern durch den Kunden Applikationen installiert und betrieben werden. Änderungsanforderungen, wie z.B. die Erweiterung des virtuellen Servers können beauftragt werden. Um einen möglichst reibungslosen Betrieb

zu erreichen, können die Veränderungen individuell terminiert werden. Mit der Beauftragung der Benutzerzahl und der Angabe der Standorte wird durch den Kunden die für den CGM Arztinformationssysteme (AIS)-Betrieb notwendigen virtuellen Maschinen (VM) mit den entsprechenden Computer-Ressourcen festgelegt und die CGM stellt diese im Rahmen der Einrichtung zu weiteren Installationszwecken bereit. Die Installation sowie die Datenmigration der CGM AIS bedürfen einer gesonderten Beauftragung eines CGM Vertriebs- und Servicepartners.

Die Integration in die lokale Praxisinfrastruktur des Kunden erfolgt durch den Kunden mit der Beauftragung eines Servicepartners.

Jeder virtuelle Server erhält mindestens eine 100 GB Systempartition die ausschließlich für das Betriebssystem genutzt werden darf. Optional können weitere Partitionen gebucht werden. Es wird dringend empfohlen, Applikationsdaten auf einer zusätzlichen Partition zu speichern.

Die für die VM aufgewendeten Computer-Ressourcen orientieren sich an der Anzahl der gleichzeitigen Benutzer bzw. Arbeitsstationen und der Praxisstandorte = Betriebsstätten. Auf Basis der offiziellen Microsoft-Empfehlungen und den CGM AIS Voraussetzungen für den Terminalserver-Betrieb, ergibt sich das dafür notwendige Anforderungsprofil.

Größen für VMs und Kundenpaket

Jedes getrennte und individuelle Kunden- Paket umfasst immer ein Minimum an VM und somit aufgeteilte Rollen. Mindestens werden die Rollen und VM umgesetzt:

VM empfohlene und benötigte Rolle

1.VM Firewall WatchGuard vFirebox

2.VM Domänencontroller

3.VM Datenbank CGM AIS

4.VM Terminalserver für Benutzer/Arbeitsplätze max. 15

Während die Computer Ressourcen bestehend aus vCPU-Cores, vRAM und vStorage bei den VM für Firewall und ersten Domänencontroller fest definiert sind, richtet sich die Ausstattung der VM für die CGM AIS Datenbank und den bzw. die Terminalserver (RDS-Hosts), nach der Anzahl der gleichzeitigen Benutzer bzw. Arbeitsplätze und nach der Größe der Datenbanken. Ebenso hat der Einsatz von Fremdsoftware Einfluss ob weitere angepasste VM genutzt werden müssen oder ob eine Erweiterung der geplanten VM ausreichen.

Leistungserweiterungen/-änderungen

Die Erweiterung und Änderung von Leistungen erfolgt auf Kundenwunsch durch die CGM. Durch die Änderungen entstehen für die zu ändernden Komponenten weitere Kosten, ggf. sind Einmalkosten für die Bearbeitung bzw. Anpassung notwendig. Die möglichen Erweiterungen und Kosten können der CGM MEDICAL IAAS vmw Preisliste

CGM MEDICAL IAAS

vmw Leistungsbeschreibung

entnommen werden.

Die Änderungen werden zu einem mit dem Kunden individuell vereinbarten Termin durchgeführt und sind abhängig von der Dauer des Umbaus sowie der Verfügbarkeit der benötigten Komponenten.

Änderungen und Erweiterungen können zu einer kurzfristigen Nichtverfügbarkeit des Systems bzw. zu einem Neustart des Systems führen. Diese geplante Ausfallzeit ist von der Verfügbarkeitsberechnung ausgenommen und wird mit Einverständnis des Kunden durchgeführt.

Einmalleistungen

Einmalleistungen (z.B. initiale Inbetriebnahme) können vom Kunden über die CGM beauftragt werden. Dafür wird ein bedarfsgerechtes, individuelles Angebot erstellt.

Datenlöschung

Bei Beendigung des Einzelauftrags werden nach 14 Tagen automatisch die Festplatten des Servers, die zugeordneten Storage-Volumes und die entsprechenden Userlaufwerke gelöscht. Eventuell vorhandene Backup-Daten werden ebenfalls gelöscht.

Optional können die Daten der Userlaufwerke auf einem mobilen Datenträger für den Kunden bereitgestellt werden. Diese Leistung muss vor Beendigung des Vertrages bei der CGM beauftragt werden. Die Bereitstellung der Userdaten wird nach Aufwand verrechnet. Der Datenträger wird über die CGM bereitgestellt und zum aktuellen Tagespreis berechnet. Der Datenträger verbleibt nach Zusendung beim Kunden.

Bei Beendigung des Rahmenvertrags wird der Zugriff auf die remote Anbindung an das CGM MEDICAL IAAS Rechenzentrum deaktiviert.

Internetanbindung und Traffic

Für alle IaaS-Pakete garantiert die CGM MEDICAL IAAS vmw eine Peak-Bandbreite von 1 Gbit/s. Der entstehende Internet-Traffic ist in allen Paketen inklusive.

Zugangsdaten/Bereitstellung

Der Kunde wird über die Fertigstellung des CGM MEDICAL IaaS vmw Pakets durch die CGM informiert. Die nötigen Zugangsdaten für die VMs werden in den Verantwortungsbereich des Kunden übergeben. Diese Zugangsdaten müssen vom Kunden gut verwahrt werden. Ein Verlust der administrativen Zugangsdaten, würde sämtliche Zugriffe darauf einschränken und es muss eine vollständige Neuinstallation durchgeführt werden. Durch ein Fehlen der administrativen Zugänge, wäre es ebenso nicht möglich, Rücksicherungen zur Datenwiederherstellung durchzuführen.

Administration

Es werden volle Administrationsrechte innerhalb der VM an den Kun-

den übertragen. Die anschließende Administration und Softwarewartung, die Lizenzierung der Systeme liegen im Verantwortungsbereich des Kunden und sind nicht Bestandteil des Produktes „CGM MEDICAL IaaS vmw“.

Die Lizenzierung der Windows Server sowie die Zugriffslizenzen für Windows Server und Terminal-Server (RDS) sind in dem IaaS-Paket enthalten.

Backup und Disaster Recovery

Regelmäßige Backups der Infrastruktur in Form von sogenannten „snapshots“ sind im CGM MEDICAL IaaS Vertrag bereits enthalten. Diese werden täglich durchgeführt und für 14 aufeinander folgende Tage gesichert. Sollte das Wiederherstellen einer Sicherung notwendig sein, so informiert der Kunde die CGM über den gewünschten Rücksicherungspunkt. Die Dauer bis zur Wiederherstellung richtet sich nach dem Service Level Agreement und der dort beschriebenen Priorität.

Sollte der Kunde zusätzliche von der CGM verwaltete Backups wünschen, so ist dies separat zu beauftragen. Des Weiteren hat der Kunde das recht darüber hinaus eigene Backup Routinen zu etablieren und diese regelmäßig durchzuführen.

3 Szenarien mit Notwendigkeit eine Backup-Rücksicherung

- (1) Beschädigung des VM Server Betriebssysteme welches ein selbstständiges Booten verhindert.
- (2) Ransom-Ware Angriff o.ä. mit Verschlüsselung oder Beschädigung von Teilen der Daten oder Datenstrukturen
- (3) Zerstörung des Rechenzentrums – sowohl Produktive IaaS Umgebung als auch Backup-Bereiche
- (4) Längerfristiger Ausfall des Internets in der Praxis
- (5) Für eine Schadens- und Risikobetrachtung ergeben sich somit folgende Fälle:

Szenario	Beschreibung Rücksicherung und Bereitstellung	Ausfall/Wiederherstellungszeiten
1.Szenario	schneller Restore und Bereitstellung der beschädigten VM aus dem Backup	Nach Meldung /Feststellung > wenige Stunden
2.Szenario	Nach Forensischer Analyse und Feststellung des Ausmaßes erfolgt	• Einbindung Cloud-Backup und Rücksicherung gezielter Dateien und Datenbank

CGM MEDICAL IAAS

vmw Leistungsbeschreibung

	Neuinstallation der VM's. (Polizei und IT-Fo-rensik Dienstleister) Danach erfolgt eine gezielte Rücksicherung einzelner Dateien, die nicht befallen wurden.	• Durch externes Fo-rensik-Team rel. lange Ausfallzeit; Rücksicherung durch Einbindung S3 Backup-Store (wenn beauftragt) wenige Stunden • Aufbau der neuen IaaS Infrastruktur = 2-4 Tage • Komplette Betriebsbereitschaft kann unter Umständen mehrere Wochen dauern
3.Szenario	Prüfung in welchem Ausmaß das der Ransomware Angriff Backup betroffen ist!	• Wenn CGM Cloud Backup-Speicher genutzt wurde; Ausfallzeit = Aufbau neuer IaaS Infrastruktur bei neuem Anbieter und Rücksicherung CGM Cloud Backup • Diese Bereitstellung kann bis zu 4 Wochen in Anspruch nehmen • Wenn kein Cloud Backup erstellt wurde, können die Daten je nach Ausmaß der Zerstörungen auch weg sein
4.Szenario	Praxis hat über längeren Zeitraum kein „brauchbares“ Internet: Einrichtung eines lokalen Servers mit Rücksicherung aus IaaS bzw. S3-Cloud Backupspeicher (wenn beauftragt wurde)	• Kundenaufwand zur Anschaffung neuer phys. Hardware • Einrichtung und Integration in Praxisstruktur inkl. Restore und Migration • Kein Datenverlust, aber Praxis kann in dem Zeitraum der Anschaffung nicht arbeiten

4 Zusatzoptionen

Dem laufenden CGM Medical IaaS vmw Vertrag können jederzeit weitere Zusatzoptionen der entsprechenden Preisliste hinzugefügt

werden, um somit den Funktionsumfang zu erweitern. Die dadurch entstehenden Mehrkosten, werden vertragsgerecht beim nächsten Zahllauf, i.d.R. ab dem Folgemonat, in Rechnung gestellt und zum SE-PA-Einzug gebracht.

5 Voraussetzungen und Mitwirkungspflichten

Für die CGM MEDICAL IaaS vmw Paket Leistungen gelten die folgenden Voraussetzungen und Mitwirkungspflichten:

- (1) Es besteht eine aktive Internetverbindung in der lokalen IT-Umgebung die entsprechend durch eine Firewall abgesichert werden muss.
- (2) Der Kunde hat administrativen Zugriff auf das CGM Medical IaaS vmw seines Pakets.
- (3) Der Kunde trägt die Verantwortung für die Datenqualität der zur Verfügung gestellten Personen- und Organisationsdaten.
- (4) Der Kunde muss die für die Einrichtung eines IaaS Pakets erforderlichen Daten zur Verfügung stellen.
- (5) Der Betrieb von Skripten oder Messtools, die die Performance dauerhaft maximal ausreizen, sind zu unterlassen. Die CGM Medical IaaS vmw behält sich vor, solche Systeme leistungsmäßig zu drosseln.
- (6) Um die Sicherheit des IaaS-Pakets nicht zu gefährden, darf der Kunden nur Software innerhalb der CGM Medical IaaS vmw betreiben, für den der jeweilige Hersteller zeitnahe und regelmäßige Sicherheitsupdates zur Verfügung stellt. Sobald eine Software, die nicht mehr durch den Hersteller unterstützt wird, muss vom Server entfernt werden. Dafür trägt der Kunde die Verantwortung.

Erklärung: eine Software ohne regelmäßige Sicherheitsupdates, stellen ein hohes Sicherheitsrisiko für die Datensicherheit da.

Trifft eine der hier beschriebenen Voraussetzungen nicht zu, ist die CGM MEDICAL IaaS nicht verpflichtet, den beschriebenen Service mit den vereinbarten Service Leveln zu erbringen.

Diese Mitwirkungspflichten werden grundsätzlich in einer Qualität erbracht, die es der CGM erlaubt, ohne Mehraufwand die vertraglichen Verpflichtungen zu erfüllen. Verzögerungen der Leistungserbringung und/oder Verletzungen der vereinbarten Service Level, die auf die Nichterfüllung der Mitwirkungspflichten durch den Kunden zurückzuführen sind oder die nicht von der CGM vertreten sind, gehen nicht zu Lasten der CGM.

6 Lizenzierung

Bei der Verwendung von Microsoft Produkten müssen in einer von mehreren Kunden gemeinsam genutzten (shared) Umgebung (Virtual Server, Virtual Windows Server) sog. Service Provider Licence Agreement (SPLA) Lizenzen eingesetzt werden.

In der Shared Umgebung müssen für alle Folgelizenzen für Micro-

CGM MEDICAL IAAS

vmw Leistungsbeschreibung

soft Produkte auch über das Betriebssystem hinaus (z. B. MS SQL, Exchange, etc.) ebenfalls SPLA-Lizenzen genutzt werden, sofern sie auf der Infrastruktur eingesetzt werden. Es darf keine Vermischung von unterschiedlichen Lizenzmodellen von Microsoft Produkten geben. Jeder Microsoft Lizenznehmer ist für die korrekte Lizenzierung verantwortlich und muss sich an die jeweiligen Lizenzbestimmungen halten (siehe auch Service Provider Use Rights unter (<https://www.microsoft.com/en-us/licensing/product-licensing/products>)).

Jeder Kunde ist für die nachhaltige und korrekte Angabe der Lizenzen (insbesondere der User-Zahlen) selbst verantwortlich.

Der Bezug der SPLA-Lizenzen erfolgt ausschließlich über die CGM MEDICAL IaaS, sowie das Reporting und die Abrechnung. Ein eigener SPLA-Vertrag ist nicht erforderlich.

Für alle eingesetzten Softwareprodukte gelten die jeweiligen Lizenzbestimmungen der Hersteller.

Durch die Beauftragung der IaaS vmw werden auch die entsprechenden EULA der Hersteller akzeptiert.

7 Service Paket

CGM Infrastructure Monitoring

Die seitens CGM bereitgestellte Infrastruktur wird permanent, 24 Stunden an 7 Tagen der Woche auf Stabilität, Performance und Sicherheit geprüft. Hierfür ist jede virtuelle Umgebung mit einem Monitoring Agent ausgestattet, welcher kontinuierlich folgende Daten überwacht:

- CPU-Auslastung
- Disk IO
- Disk-Kapazität
- Speicher und Auslagerungsdatei
- Netzwerkschnittstellen
- Systemzeit
- Systemupdates
- Betriebszeit
- Updatestatus zur Antiviren Software

Vulnerability Scans

CGM führt wöchentliche Vulnerabilitätsscans für öffentliche (externe) IP-Adressen der Infrastruktur durch. Hierbei wird die Infrastruktur auf Sicherheitslücken wie zum Beispiel Fehlkonfigurationen oder aber vorhandene Malware, geprüft. Der Kunde wird über vorhandene Sicherheitslücken informiert und ist zur Behebung dieser verpflichtet. Hinweise um die Sicherheitslücken zu schließen werden von CGM geliefert. Sollten kritische Sicherheitslücken nach mehrfachem Hinweis durch den Kunden nicht geschlossen werden, so behält sich die CGM das Recht vor die Infrastruktur bis zur Behebung der Sicherheitslücken zu deaktivieren. In diesem Fall muss aufgrund der fehlenden Konnektivität

die Behebung der Sicherheitslücken entgeltlich durch die CGM erfolgen.

Servicezeiten und Kontaktdetails

Eine telefonische Anruf-Annahme erfolgt innerhalb der Bürozeiten der CGM über die bekannten Rufnummern.

Incident Management

(Unterbrechung des Service/technischer Defekt)

Im Falle eines Incidents wird der Service Desk Mitarbeiter die technische Diagnose durchführen und versuchen mit Hilfe einer Knowledge Datenbank sofort eine Lösung zu finden. Die erfolgreiche Lösung sowie die durchgeführten Lösungsschritte werden dokumentiert und nach Beseitigung der Störung wird der Incident geschlossen. Der Kunde wird über die Behebung der Störung informiert. Sollte eine sofortige Lösung nicht möglich sein, werden alle bisherigen Maßnahmen dokumentiert und der Vorgang an nachgelagerte Instanzen (2nd Level Support) weitergeleitet. Bei einer Weiterleitung wird der Incident vom Service Desk über die gesamte Service Zeit proaktiv überwacht, um anhand eines definierten Eskalationsprozesses die Einhaltung der vereinbarten Service Level sicherzustellen. Nach erfolgreicher Lösung eines Incidents und Schließung des Tickets im System wird der Kunde darüber informiert.

8 SLA

Die CGM MEDICAL IAAS vmw garantiert im Bereich CGM MEDICAL IAAS IaaS eine Verfügbarkeit von Netzwerk, Stromversorgung und Klimatisierung von 99,95 % zum Jahresmittel. Die garantierte Verfügbarkeit der CGM MEDICAL IaaS Systeme liegt bei 99,90 % zum Jahresmittel.

Service Level

Die Vereinbarung von Service Level Agreements (SLA) bildet eine vertragliche Basis zwischen dem Auftraggeber und der CGM bzgl. der Leistungserbringung der IaaS Leistungen.

Bediente Service-Zeit: **Mo-Fr 8:00-18:00 Uhr** (Hotline Erreichbarkeit)

Service Level Verfügbarkeit:

Die Service Level Verfügbarkeit wird pro Jahresmittel für die bereitgestellte Leistung gemessen.

Um eine Wartung der zugrundeliegenden Systeme durch die CGM zu ermöglichen sind unterschiedliche Wartungsfenster definiert:

- Damit ein konsistentes Backup erfolgen kann, wird jeden Tag zwischen 23 Uhr und 4 Uhr die Datenbank heruntergefahren und anschließend wieder gestartet. In dieser Zeit kann mit dem CGM AIS nicht gearbeitet werden.
- Geplante Wartungsfenster mit Einschränkungen der vertraglich

CGM MEDICAL IAAS

vmw Leistungsbeschreibung

definierten Service Verfügbarkeiten: Mo.–Fr.: 18:30 – 22:30 Uhr, Sa.: 8:00 – 14:00 Uhr Diese werden fünf [5] Kalendertage vorher angekündigt.

- Die Zeiten der genutzten Wartungsfenster fließen nicht in die Berechnung der Serviceverfügbarkeit ein.

Die CGM MEDICAL IaaS kann dringende Änderungen an der Software und/oder den Hardware-Systemen außerhalb der Wartungsfenster durchführen, wenn diese bei Unterlassen der Änderungen zu einer Beeinträchtigung der vereinbarten Verfügbarkeit führen. Diese Änderungen erfordern darüber hinaus eine besondere Erklärung der Dringlichkeit.

Die Verfügbarkeit eines IaaS Servers gilt als gegeben, wenn die entsprechende Serverinfrastruktur aus dem Netz der CGM MEDICAL IaaS erreichbar ist bzw. das Betriebssystem läuft. Die Messung der Verfügbarkeit erfolgt auf Basis der Performance- und Statusüberwachung der Serversysteme.

Ein IaaS Paket gilt als betriebsfähig bereitgestellt, wenn dem Kunden durch die CGM die Freischaltung des Zugangs mitgeteilt wurde. Entsprechend der Bestellung werden zu diesem Zeitpunkt ggf. die Administrationsrechte übergeben.

9 Sonstige Bestimmungen

Leistungen, die hier nicht beschrieben sind, können individuell beim Service-Partner gesondert beauftragt werden.