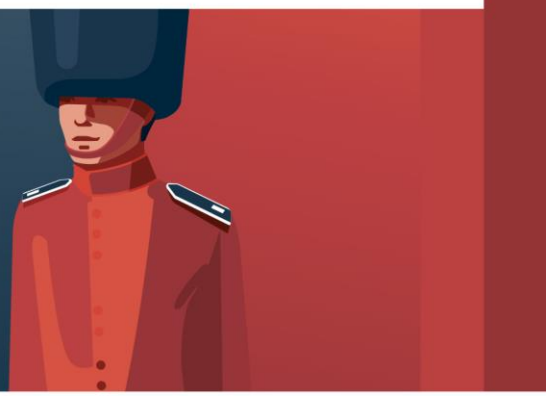
DataGuard



16.12.2022

# ANLAGE 1

## TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN
## i.S.d Art.32 DS-GVO

Auftragnehmer: x-cellent technologies GmbH

## Zutrittskontrolle

**Unternehmen x-cellent:**
**Zutrittskontrollsystem - Abschließbare Räume:**
Im Unternehmen sind sämtliche Räume, in denen ein Zugriff auf personenbezogene Daten möglich ist, abschließbar.
**Zutrittskontrollsystem - Besucher:**
Im Unternehmen werden Besucher stets begleitet und abgeholt.
**Zutrittskontrollsystem:**
Im Unternehmen wird ein zentral verwaltetes Zutrittskontrollsystem eingesetzt.
**Server - Externer Einsatz:**
Im Unternehmen werden externe Server (z.B. in einem Rechenzentrum) angemietet.
**Server:**
In den Unternehmensräumlichkeiten werden ein oder mehrere Server eingesetzt.
**Server - Räumlichkeiten:**
Die im Unternehmen eingesetzten Server werden in einem speziell dafür vorgesehenem Raum betrieben.
**Server - Zutrittskontrolle:**
Im Unternehmen wird ein Zutrittskontrollsystem zum Serverraum eingesetzt.
**Server - Zutrittsberechtigung:**
Im Unternehmen ist der Zutritt zu den Serverräumen auf den minimal benötigten Personenkreis beschränkt.
**Sicherung des Unternehmensgeländes - Abgrenzung:**
Das Unternehmensgelände / die Unternehmensräumlichkeiten werden vom öffentlichen Bereich abgegrenzt durch:
- Büro in größerem Gebäudekomplex
- Abschließbare Tür

**Zutrittskontrollsystem - Technisches Mittel:**
Das Zutrittskontrollsystem basiert auf folgenden technischen Mitteln:
- Schlüssel
- Token/Transponder mit Sicherheitsfunktion

**Zutrittskontrollsystem - Verwaltung:**
Das Zutrittskontrollsystem wird folgendermaßen verwaltet:
- Schlüsselbuch
- Elektronisch

**Produkt Metal Stack Cloud**
**Zutrittskontrollsystem - Abschließbare Räume:**
Rechenzentrum: Modernes Rechenzentrum mit abgeschlossenen Cages
**Zutrittskontrollsystem - Besucher:**
Rechenzentrum: Besucher haben grundsätzlich keinen Zutritt zum Cage.
**Zutrittskontrollsystem:**
Jeder Zutritt zum Rechenzentrum muss im Vorfeld per Website genehmigt werden.Es wird der Personalausweis verlangt und ein biometrischer Faktor genommen welcher zum Verlassen der Serverräume notwendig ist.
**Server - Räumlichkeiten:**
Die eingesetzten Server werden in einem speziell dafür vorgesehenem Raum im Rechenzentrum betrieben.
**Server - Zutrittskontrolle:**
Im Rechenzentrum wird ein Zutrittskontrollsystem zum Serverraum und dem jeweiligen Cage eingesetzt.
**Server - Zutrittsberechtigung:**
Im Rechenzentrum ist der Zutritt zu den Serverräumen und den entsprechenden Cages nur Metal Stack CloudAdministratoren nach Genehmigung und Anmeldung für eine beschränkte Dauer gestattet.
**Sicherung des Rechenzentrums - Abgrenzung:**
Das Rechenzentrum wird vom öffentlichen Bereich abgegrenzt durch:
Zaun mit Drehkreuz (Vereinzelungsanlage), Kameraüberwachung außerhalb des Gebäudes, Gebäudezutritt gesichert durch Wechselsprechanlage und Sicherheitspersonal welches 24/7 vor Ort ist
**Zutrittskontrollsystem - Technisches Mittel:**
Das Zutrittskontrollsystem verwendet folgende technischen Mittel:
2 Faktor Authentifizierung (Zugangsausweis und biometrischer Faktor)

**Rechenzentrum Zutrittskontrollsystem - Gebäudesicherung**
Alle Zu- und Ausgänge des Rechenzentrums werden durch ein Geländeüberwachungssystems ständig kontrolliert.
**Rechenzentrum Zutrittsorganisation – Serverbereich (Colocation-Bereichs)**
Zugangsautorisierung und Validierung für Besucher durch Kundenadministratoren und Sicherheitspersonal, Sicherheitsschleusen, biometrische Lesegeräte und Zugangsausweislesegeräte, Schließfachschränke und umfangreiche Überwachung per Video und/oder durch das Personal des Rechenzentrums vor Ort.

## Datenträgerkontrolle

**Unternehmen x-cellent:**
**Datenträgermanagement - Schreddern von Akten:**
Im Unternehmen werden Akten geschreddert.
**Datenträgermanagement - Zugriffsschutz:**
Im Unternehmen werden zur Entsorgung gesammelte schutzbedürftige Datenträger vor unberechtigtem Zugriff geschützt.
**Tragbare Datenträger - Verschließbare Behältnisse:**
Im Unternehmen stehen an allen Arbeitsplätzen verschließbare Behältnisse zur Verfügung, um Unterlagen und Datenträger sicher aufbewahren zu können.
**Tragbare Endgeräte - Diebstahlsicherung:**
Im Unternehmen werden tragbare Endgeräte außerhalb der Nutzungszeiten gegen Diebstahl gesichert.
**Datenträgermanagement - Verschlüsselung:**
Im Unternehmen werden elektronische Datenträger verschlüsselt.
**Datenträgermanagement - Bestandsverzeichnis:**
Im Unternehmen wird für folgende elektronischen Datenträger ein Bestandsverzeichnis geführt:
- Laptops
- Mobiltelefone

**Datenträgermanagement - Sicherheitsstufe für Entsorgung:**
Im Unternehmen wird folgende Sicherheitsstufe bei Aktenvernichtern verwendet:
- 4

**Datenträgermanagement - Entsorgungsregeln:**
Im Unternehmen wurden für folgende Datenträger Entsorgungsregeln definiert:
- Festplatten
- Akten

**Datenträgermanagement - Verschlüsselungsverfahren:**
Im Unternehmen werden folgende Verschlüsselungsverfahren für Datenträger verwendet:
- dm-crypt, Bitlocker

**Produkt Metal Stack Cloud**
**Verschlüsselung von Datenträgern?**
Es existiert keine Verschlüsselung auf Storageebene. Der Kunde kann auf Applikationsebene seine eigene Verschlüsselung anwenden.
**Abgeschlossene/sichere Lagerung von Datenträgern.**
Ausgediente Datenträger werden vor der professionellen Entsorgung in einer Box innerhalb des Cages im Rechenzentrum gelagert.

## Speicherkontrolle

**Unternehmen x-cellent:**
**Mitarbeiter - Fachgerechte Entsorgung personenbezogener Daten:**
Im Unternehmen sind die Beschäftigten angehalten personenbezogene Daten fachgerecht zu entsorgen.
**Passwortschutz - Passwortliste:**
Es wird keine unverschlüsselte Passwortliste geführt.
**Passwortschutz - Protokollierung von Falscheingaben:**
Falscheingaben des Passworts werden protokolliert.
**Automatische Bildschirmsperre:**
Im Unternehmen wird eine automatische Bildschirmsperre eingesetzt.
**Automatische Bildschirmsperre - Zeitraum:**

Im Unternehmen wird die automatische Bildschirmsperre nach maximal 10 Minuten aktiviert.
**Authentifizierung - Datensperrung und -löschung:**
Im Unternehmen besteht die Möglichkeit auf Antrag personenbezogene Daten zu sperren und zu löschen.
**Authentifizierung - Benutzerauthentifizierung IT-Systeme:**
Zur Benutzerauthentifizierung in IT-Systemen werden folgende Verfahren verwendet:
- Passwort

**Produkt Metal Stack Cloud:**
Pseudonymisierung und Anonymisierung finden nicht statt da die Datenhoheit dem Kunden obliegt.
**Sonstige ergriffene Massnahmen**
Mandantentrennung auf Serverebene und Storageebene
Professionelle Entsorgung von Datenträgern durch ein externes Unternehmen.

## Zugangskontrolle

**Unternehmen x-cellent:**
**Tragbare Endgeräte - Zugangssperren:**
Im Unternehmen verfügen tragbare Endgeräte über Zugangssperren (Passwort, PIN, Muster o. A.).
**Fernwartung - VPN:**
Im Unternehmen wird zur Fernwartung ein VPN-Tunnel eingesetzt.
**Fernwartung - Sicherheitsmaßnahmen:**
Im Unternehmen wird die Fernwartung unter angemessenen Sicherheitsmaßnahmen durchgeführt.
**Fernwartung - Zugangsmöglichkeiten:**
Im Unternehmen werden Fernwartungszugänge individuell freigegeben.
**Passwort-Manager:**
Im Unternehmen wird ein Passwort-Manager eingesetzt.
**Passwort-Manager - Zugangskontrolle:**
Der eingesetzte Passwort-Manager bietet eine ausreichende Zugangskontrolle und eine verschlüsselte Speicherung.
**Authentifizierung - Zwei-Faktor-Authentifizierung:**
Im Unternehmen wird eine Zwei-Faktor-Authentifizierung eingesetzt.
**Zugang zu personenbezogenen Daten in Bereichen mit Publikumsverkehr:**
Im Unternehmen wird dafür gesorgt, dass personenbezogene Daten in Bereichen mit Publikumsverkehr nicht frei zugänglich sind.

**Fernwartung - Tools:**
Im Unternehmen werden folgende Tools zur Fernwartung eingesetzt:
- TLS-Verschlüsselt
- TeamViewer
- Remote Desktop Control

**Produkt Metal Stack Cloud**
**Authentifizierung von Benutzern**
Authentifizierung von Benutzern erfolgt über OAuth. Die Benutzeridentitäten werden auf Grundlage einer bestehenden, verifizierten Authentifizierung des Kunden bestätigt.

**Passwortrichtlinien/Passwortkomplexität)**
Passwortrichtlinien und Passwortkomplexität sind durch jeweiligen OAuth Provider vorgegeben.

**2 Faktor Authentifizierung**
2 Faktor Authentifizierung wird durch den OAuth Provider gefordert und umgesetzt.

### Sperrung Systemzugang nach definierter Anzahl von Falschanmeldungen

Ob und wann ein Zugang gesperrt wird liegt in der Verantwortung des OAuth Providers.

## Zugriffskontrolle

**Unternehmen x-cellent:**
**IT-Sicherheit - Firewall:**
Im Unternehmen wird eine bzw. mehrere Firewalls gegen unerwünschte Netzwerkzugriffe eingesetzt.
Im Unternehmen werden folgende Firewalls eingesetzt:
- SonicWall, iptables

**Vergabe von Zugangs- und Zugriffsberechtigungen:**
Im Unternehmen erfolgt die Vergabe von Zugangs- und Zugriffsberechtigungen anhand der Funktion der Zugangs- bzw. Zugriffsberechtigten. Für individuelle Berechtigungen ist ein Autorisierungsprozess implementiert: Nachdem Einzelberechtigungen beantragt werden, müssen diese von der verantwortlichen Führungskraft freigegeben werden, bevor die IT diese freischaltet. In der Berechtigungsstruktur wird das Need-to-Know Prinzip und eine strikte Funktionstrennung beachtet.

**Produkt Metal Stack Cloud:**
**Rollenbasiertes Berechtigungsmanagement**
Ein rollen-basiertes Berechtigungsmanagement regelt den Zugriff auf Worker Nodes.
Der Zugriff auf Controlplane ist nur qualifizierten Metalstack Cloud Administratoren gestattet.
Administrative Rollen werden von den jeweiligen Ownern zugewiesen.
**Sonstige ergriffene Maßnahmen:**
Mandantentrennung auf Storageebene anhand des Projektnamens.

## Benutzerkontrolle

**Unternehmen x-cellent:**
**Telekommunikation - Datenschutz für Mobile Arbeiter:**
Mobile Arbeiter wurden auf die Einhaltung einschlägiger Datenschutzvorschriften hingewiesen.
**Administratoren:**
Im Unternehmen wurde für alle IT-Systeme und IT-Netze Administratoren sowie deren Stellvertreter bestimmt.
**Administratoren - Spezielle Konten:**
Im Unternehmen werden spezielle Administratorenkonten eingesetzt.
**IT-Sicherheit - Administratoren Qualifikation:**
Im Unternehmen wird sichergestellt, dass IT-Administratoren über ausreichende Qualifikation zur Ausübung ihrer Tätigkeit besitzen.
**Mitarbeiter - Maßnahmen:**
Um im Unternehmen die Beschäftigten auf die Wichtigkeit des Datenschutzes hinzuweisen und diese gemäß den Erfordernissen zu verpflichten, werden folgende Maßnahmen
getroffen:
- Verpflichtung der Beschäftigten zu Verhaltensregeln
- Information der Mitarbeiter über Neuerungen zum Thema Datenschutz
- Unternehmensinterne Datenschutz-Richtlinien
- Verpflichtung der Beschäftigten auf das Datengeheimnis

**Administratoren - Ebenen:**
Im Unternehmen werden die Administratorenkonten auf folgender Ebene eingesetzt:
- Betriebssystem

**Produkt Metal Stack Cloud:**
### Sonstige ergriffene Maßnahmen
Der Kunde kann nur diejenigen Daten bearbeiten welche ihm gehören. Bedingt durch die physikalische Mandantentrennnung hat ein Kunde keine Möglichkeit auf ihm nicht gehörende Daten zuzugreifen.

## Transportkontrolle

**Unternehmen x-cellent**
**Datenübertragung - Verschlüsselung der Datenträger:**
Im Unternehmen werden Datenträger verschlüsselt, welche übermittelt werden sollen.
**Datenübertragung - Berechtigter Zugriff:**
Im Unternehmen werden beschriebene Datenträger vor und nach dem Versand so aufbewahrt, dass ein Zugriff nur für berechtigte Personen möglich ist.
**Datenübertragung - Unkenntlicher Transport:**
Im Unternehmen werden Behältnisse, die dem Transport von Datenträgern mit personenbezogenen Daten dienen, nicht als solche beschriftet.
**Datenübertragung - Verschlüsselung:**
Daten werden bei der Übertragung mit den folgenden Verfahren/Protokollen verschlüsselt:
- SSL/TLS

**Produkt Metal Stack Cloud**
### Sonstige ergriffene Maßnahmen
Eine physikalische Datenübertragung findet nur im Rahmen der Entsorgung statt.

## Übertragungskontrolle

**Unternehmen x-cellent:**
**VPN-Tunnel:**
Im Unternehmen wird ein VPN-Tunnel zur Datenübertragung eingesetzt.
**VPN-Tunnel - Firewall:**
Im Unternehmen wird zusätzlich eine Firewall für den VPN-Tunnel eingesetzt.
**Telekommunikation - Verbindung zum Telekommunikationsprovider:**
Zur Verbindung mit dem Telekommunikationsprovider wird folgende Methode verwendet:
- Standleitung
- Reguläre DSL/Glasfaserverbindung

**VPN-Tunnel - Endpunkt Platzierung:**
Der VPN-Tunnel Endpunkt ist an folgender Stelle platziert:
- In der Firewall

**Produkt Metal Stack Cloud**
### Verschlüsselung für kritische Daten bei der Datenübertragung
Kuberneteszugriffe sind generell TLS verschlüsselt.
Die Secrets der Kubernetescluster sind generell verschlüsselt.
Der Kunde trägt die Verantwortung durch die Gestaltung seiner Systemlandschaft.

## Wiederherstellbarkeit

**Unternehmen x-cellent**
**Sicherungen - Unternehmensweite Richtlinie:**
Im Unternehmen gibt es eine unternehmensweite Richtlinie zu Sicherungen.
**Sicherungen - Schriftliche unternehmensweite Richtlinie:**
Im Unternehmen gibt es eine schriftlich definierte unternehmensweite Richtlinie zu Sicherungen.
**Sicherungen - Umsetzung:**
Im Unternehmen wird die Richtlinie zu Sicherungen auch in der Praxis umgesetzt.
**RAID-System:**
Im Unternehmen wird ein RAID-System eingesetzt.
**Sicherungen - Wiederherstellungsmöglichkeiten:**
Im Unternehmen können folgende Bereiche wiederhergestellt werden:
- Installationen
- Systemdateien- und Datencontainer
- Log-Daten

- Benutzerkonten
- Konfigurationen (Einstellungen und Freigaben)
- Daten

**RAID-System - Level:**
Im Unternehmen wird folgendes RAID Level eingesetzt:
- RAID 6

**Sicherungen - Sicherungsarten:**
Im Unternehmen werden folgende Sicherungsarten eingesetzt:
- Inkrementelle Sicherung
- Komplett-/Vollsicherung

**Sicherungen - Sicherungsmedien:**
Im Unternehmen werden die folgenden Speichermedien für Sicherungen verwendet:
- Festplatte
- Cloud Storage Boxen

**Sicherungen:**
Im Unternehmen werden die Sicherungen durchgeführt von:
- Eigenständige Backups (z. B. durch NAS-System)

**Produkt Metal Stack Cloud**

### Datensicherungskonzept (Backup-Konzept) inkl. regelmäßige Sicherungen

Alle Daten der Controlplane werden im 3 Minuten-Takt gesichert

### Disaster-Recovery-Plan (DRP) / Notfallplan

Es findet ein automatischer Restore der ggf. verlorenen Daten der Controlplane statt.
Die Controlplane  ist redundant in zwei Rechenzentren aufgebaut.

## Zuverlässigkeit

**Unternehmen x-cellent**

**IT-Sicherheit - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**
Im Unternehmen wird ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung eingesetzt.

**IT-Sicherheit - Software zur Netzwerküberwachung:**
Im Unternehmen wird eine Software zur Überwachung des Netzwerks bzw. der Anwendungen verwendet.
Im Unternehmen wird folgende Software zur Überwachung des Netzwerks bzw. der Anwendungen eingesetzt:
- Nagios, Grafana

**IT-Sicherheit - Schutz vor Schadsoftware**
Auf allen relevanten Systemen sind aktuelle Virenscanner implementiert.

**IT-Sicherheit - Software Aktualisierungen:**
Aktualisierungen werden zeitnah wie folgt umgesetzt:
- Manuell

**Produkt Metal Stack Cloud**

### Netzwerküberwachung / Intrusion Detection System (IDS / IPS)

IDS für jeden Kundencluster auf der Firewall des Kunden
Ein IDS System wird automatisch bei der Erstellung eines Clusters mit einer Firewall aufgesetzt.

### Changemanagement

Nur qualifizierte MetalStack Cloud Administratoren dürfen Änderungen die über ein Ticket dokumentiert sind an der Plattform durchführen.

### Aktualisierungen (Updates) bzw. Patch- und Schwachstellenmanagement

Automatische Updates für die Betriebssysteme der Kundencluster sowie für die Kubernetesversionen der Kundencluster werden bereitgestellt.
Automatische Updates von Betriebssystem und Kubernetesversion der Controlplane werden durchgeführt.

### Sonstige ergriffene Maßnahmen

Überprüfung der Funktionsfähigkeit oben genannter automatischer Updates im Rahmen von

automatisierten Integrationstests.

## Verfügbarkeitskontrolle

**Unternehmen x-cellent:**
**Unterbrechungsfreie Stromversorgung :**
Im Unternehmen wird eine unterbrechungsfreie Stromversorgung eingesetzt.
**Unterbrechungsfreie Stromversorgung - Überprüfung nach Änderungen:**
Im Unternehmen wird die Leistung der unterbrechungsfreien Stromversorgung erneut geprüft, wenn Änderungen an der Hardware vorgenommen wurden.
**Archivierungskonzept:**
Im Unternehmen wurde ein Archivierungskonzept definiert, welches regelt, wie und wie lange Dokumente archiviert werden.
**Archivierungskonzept - Gesetzliche Aufbewahrungspflicht:**
Es liegt eine gesetzliche Aufbewahrungspflicht für die archivierten Dokumente vor.
**Unterbrechungsfreie Stromversorgung - Überbrückungsdauer:**
Die unterbrechungsfreie Stromversorgung kann folgenden Zeitraum überbrücken:
- 30 Minuten
**Server - Gefahrenabsicherung:**
Die Serverräume wurden gegen folgende Gefahren abgesichert:
- Überhitzung
- Stromausfall

**Produkt Metal Stack Cloud**
### Gewährleistung des Betriebs bei Störung der Energieversorgung
**Redundanter Strom**:
Elektrizität wird über zwei (2) Stromkreise von zwei verschiedenen Energiequellen geliefert.
### Redundante Auslegung sämtlicher wichtigen Systeme:
Bei Ausfall eines Servers in einem Kubernetescluster eines Kunden wird automatisch ein neuer Server gestartet.
**RAID System**
Kundendaten werden über drei voneinander unabhängigen Storagesystemen gespiegelt
### Schutz vor Feuer im Serverraum
Das Rechenzentrum bietet modernsten Brandschutz und ist gemäß der Norm DIN EN 50600 aufgebaut.
### Schutz vor Überhitzung der Server
Die Server werden innerhalb des Rechenzentrums gekühlt. Die Kühlung ist 24/7 in Betrieb und gegen Ausfälle geschützt.
### Sonstige ergriffene Maßnahmen
**Klimakontrolle**:
Luftfeuchtigkeit und Temperatur werden kontinuierlich überwacht und geregelt.

## Auftragskontrolle

**Unternehmen x-cellent:**
**Externe Dienstleister:**
Das Unternehmen arbeitet mit externen Dienstleistern zusammen.
**Externe Dienstleister - Kontakt zu personenbezogenen Daten:**
Im Unternehmen werden externe Dienstleister, welche in Kontakt mit personenbezogenen Daten gelangen könnten, stets bei der Tätigkeit überwacht.
**Externe Dienstleister - Weisungen zur Verarbeitung:**
Im Unternehmen werden Weisungen zur Verarbeitung personenbezogener Daten ausschließlich schriftlich an Auftragsverarbeiter erteilt.
**Dienstleister Datenträgerentsorgung:**
Es wird ein externer Dienstleister zur Entsorgung von Datenträgern genutzt.
**Dienstleister Datenträgerentsorgung - Zertifizierung:**
Der externe Dienstleister besitzt folgende Zertifizierung:
- DIN EN ISO 9001:2015

**Produkt Metal Stack Cloud**

### Auswahl der Auftragnehmer unter Sorgfalt-Gesichtspunkten

Es werden nur Rechenzentren gewählt welche nach gängigen Normen aufgebaut sind (DIN EN50600).

**Entsorgung von Datenträgern**

Die Verwaltung von Datenträgern inkl. Entsorgung ist nicht Aufgabe des Rechenzentrums.
Eine professionelle Drittfirma wird damit beauftragt die Entsorgung unter Aufsicht eines Metalstack Cloud Administrators durchzuführen.

**Regelungen zu Fremdpersonal**

Der Zugang und Zugriff ist Fremdpersonal nicht gestattet und weder technisch noch physikalisch möglich.

## Datenintegrität

**Unternehmen x-cellent:**
Keine gesonderten TOMs

**Produkt Metal Stack Cloud**

### Sonstige ergriffene Maßnahmen

Das Risiko von mangelhafter Datenintegrität aufgrund fehlerhafter Hardware wird durch Spiegelung der Storagesysteme minimiert.

## Nachvollziehbarkeit

**Unternehmen x-cellent:**
Keine gesonderten TOMs

**Produkt Metal Stack Cloud**

**Protokollierung von Zugriffsversuchen auf IT Systeme**

API Zugriffe der Kunden werden protokolliert.

**Protokollierung von Aktivitäten auf dem Server**

Das Auditing der Controlplane ist aktiviert. Protokolldateien werden für den Zeitraum von einem Monat aufbewahrt.

## Trennbarkeit

**Unternehmen x-cellent:**
Keine gesonderten TOMs

**Produkt Metal Stack Cloud**

### Trennung des WLAN in privat und öffentlich

Im Rechenzentrum gibt es kein WLAN, daher entfällt die Unterscheidung zwischen privat und öffentlich.

### Trennung in Test-, Produktions- und Entwicklungsebene

Im Rechenzentrum ist eine Trennung in verschiedene IT-Umgebungen nicht vorgesehen.
Jedes Deployment der Metal Stack Cloud durchläuft eine DevOps Pipeline. Während des Durchlaufes wird das neue Deployment getested. Erst wenn diese Tests alle positiv ausfallen wird das Deployment für die Produktion bereitgestellt.

### Trennung von Datenverarbeitungen (logisch oder physikalisch), Mandantenfähigkeit

Kundencluster basieren auf  dedizierter Hardware für jeden Kunden. Eine Mandantentrennung ist daher implizit gegeben.

Das Storagesystem beinhaltet eine eingebaute Mandantentrennung.