



**Technische und  
organisatorische  
Massnahmen  
(TOM)**

## **Inhaltsverzeichnis**

Zutrittskontrolle Rechenzentren	<b>3</b>
Zugangskontrolle	<b>4</b>
Zugriffskontrolle	<b>5</b>
Trennungskontrolle	<b>5</b>
Weitergabekontrolle	<b>6</b>
Verfügbarkeits- und Belastbarkeitskontrolle	<b>6</b>
Regelmässige Überprüfung, Bewertung und Evaluierung	<b>7</b>
Security Incident Response Management	<b>8</b>
Datenschutzfreundliche Voreinstellungen: Privacy by design / Privacy by default	<b>8</b>



**Technische und  
organisatorische  
Massnahmen  
(TOM)**

## **Informationssicherheits- und Datenschutz Standards – technische und organisatorische Massnahmen (TOM)**

### **Für alle Auftragsverarbeitungen gemäss Art. 9 DSGVO**

MOUNT10 gewährleistet im Interesse der Integrität, Nachvollziehbarkeit, Verfügbarkeit und Vertraulichkeit der verarbeiteten Personendaten mit geeigneten technischen und organisatorischen Massnahmen (TOM) eine dem Risiko angemessene Datensicherheit.

Der Kunde überlässt MOUNT10 im Rahmen der vereinbarten Verträge und AGB in seinem eigenen Ermessen und in seinem Auftrag Personendaten und/oder geheimnisgebundene Daten zur Bearbeitung. Diese Massnahmen finden Anwendung auf alle Tätigkeiten, die mit der Dienstleistung in Zusammenhang stehen und bei denen Mitarbeitende des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Die aktuellen TOM finden Sie unter: <https://mount10.ch/tom/>



**Technische und  
organisatorische  
Massnahmen  
(TOM)**

**Zutrittskontrolle Rechenzentren**

(Massnahmen zur Verhinderung von Zutritten Unberechtigter zu Datenverarbeitungsanlagen)

<b>Technische Massnahmen</b>	<b>Organisatorische Massnahmen</b>
<ul style="list-style-type: none"><li>✓ Vereinzelungsanlagen</li><li>✓ Videoüberwachung</li><li>✓ elektronisches Schliesssystem mit Berechtigungsmanagement</li><li>✓ Alarmsystem</li><li>✓ Sicherheitsschlösser</li></ul>	<ul style="list-style-type: none"><li>✓ Personenidentifikation</li><li>✓ Protokollierung der Zutritte</li><li>✓ vertragliche Absicherung (NDA) mit Dienstleistern (Wartung)</li><li>✓ Sorgfältige Auswahl von Personal und Lieferanten</li><li>✓ Ausweise für Mitarbeitende und Gäste</li><li>✓ Wachpersonal</li><li>✓ Restriktive Zugangsrichtlinien</li><li>✓ Besucherbegleitung ausschliesslich durch berechnigte Mitarbeitende</li></ul>



**Technische und  
organisatorische  
Massnahmen  
(TOM)**

**Zugangskontrolle**

(Massnahmen zur Verhinderung des Zugangs Unberechtigter zu Datenverarbeitungsanlagen)

<b>Technische Massnahmen</b>	<b>Organisatorische Massnahmen</b>
<ul style="list-style-type: none"><li>✓ Personen-Authentifikation</li><li>✓ Zwei-Faktor Authentifizierung (2FA)</li><li>✓ Einsatz Firewall-Cluster</li><li>✓ Einsatz von VPN-Technologien</li></ul>	<ul style="list-style-type: none"><li>✓ Berechtigungskonzept</li><li>✓ regelmässige Überprüfung der Benutzerberechtigungen</li><li>✓ zentrales Passwort-Management</li><li>✓ Passwortrichtlinien</li><li>✓ Protokollierung von Zugriffen</li><li>✓ Richtlinie IT-Nutzung für Mitarbeitende</li><li>✓ Home-Office Weisung</li><li>✓ Umfassende Sensibilisierung und stetige Fortbildung der Mitarbeitenden im Bereich Cyber-Security und Datenschutz</li></ul>



**Technische und organisatorische Massnahmen (TOM)**

**Zugriffskontrolle**

(Berechtigte dürfen ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können – need-to-know Prinzip)

Technische Massnahmen	Organisatorische Massnahmen
<ul style="list-style-type: none"> <li>✓ Protokollierung von Zugriffen</li> <li>✓ Professionelle physische Vernichtung von Datenträgern</li> </ul>	<ul style="list-style-type: none"> <li>✓ Minimale Anzahl Administratoren</li> <li>✓ Verwalten von Benutzerberechtigungen durch Administratoren</li> <li>✓ Accounts der austretenden Mitarbeitenden werden umgehend deaktiviert</li> </ul> <p>Alle Administrationszugriffe werden protokolliert</p>

**Trennungskontrolle**

(Zu unterschiedlichen Zwecken erhobene Personendaten müssen getrennt verarbeitet werden können)

*Die MOUNT10 AG hat keinen Zugriff auf die Kundendaten, da diese mit dem Schlüssel des Kunden verschlüsselt sind*

Technische Massnahmen	Organisatorische Massnahmen
<ul style="list-style-type: none"> <li>✓ Physikalische und virtuelle Trennung (Systeme / Datenbanken / Storage)</li> <li>✓ Trennung von Produktiv- und Testumgebung</li> <li>✓ Mandantenfähigkeit relevanter Anwendungen</li> </ul>	<ul style="list-style-type: none"> <li>✓ Berechtigungs- und Zugriffskonzept</li> <li>✓ Restriktives Berechtigungskonzept</li> </ul>



**Technische und organisatorische Massnahmen (TOM)**

**Weitergabekontrolle**

Massnahmen, die gewährleisten, dass Daten während ihres Transports oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

*Die MOUNT10 AG hat keinen Zugriff auf die Kundendaten, da diese mit dem Schlüssel des Kunden verschlüsselt sind*

Technische Massnahmen	Organisatorische Massnahmen
<ul style="list-style-type: none"> <li>✓ Verschlüsselte Übertragung der Daten</li> <li>✓ Verschlüsselte Speicherung der Daten</li> <li>✓ keine Weitergabe von pseudonymisierten Daten an Dritte</li> </ul>	<ul style="list-style-type: none"> <li>✓ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. Löschfristen gemäss AGB</li> </ul>

**Verfügbarkeits- und Belastbarkeitskontrolle**

Technische Massnahmen	Organisatorische Massnahmen
<ul style="list-style-type: none"> <li>✓ Unterbrechungsfreie Stromversorgung (USV)</li> <li>✓ Schutz gegen Feuer, Rauch, Überflutungen, Feuchtigkeit etc.</li> <li>✓ Klimaüberwachung der Server Räume</li> <li>✓ Notstrom-Generator</li> <li>✓ Redundante Stromversorgung</li> <li>✓ Redundanter Storage</li> <li>✓ Videoüberwachung</li> <li>✓ Alarmanlage</li> <li>✓ Monitoring-Systeme</li> </ul>	<ul style="list-style-type: none"> <li>✓ Backup-Konzept</li> <li>✓ Business Continuity Management (BCM)</li> <li>✓ Prüfung des Wiederherstellung-Prozesses</li> <li>✓ Regelmässige Überprüfung und Tests der Notfallpläne</li> <li>✓ Security Incident Management Weisung</li> </ul>



**Technische und  
organisatorische  
Massnahmen  
(TOM)**

**Regelmässige Überprüfung, Bewertung und Evaluierung**

<b>Technische Massnahmen</b>	<b>Organisatorische Massnahmen</b>
<ul style="list-style-type: none"><li>✓ Zugriff der Mitarbeitenden auf interne Weisungen</li></ul>	<ul style="list-style-type: none"><li>✓ Datenschutzberater DSB (extern)</li><li>✓ Informationssicherheitsbeauftragter CISO (extern)</li><li>✓ Schulung der Mitarbeitenden im Bereich Cyber-Security und Datenschutz</li><li>✓ Regelmässige Überprüfung der Wirksamkeit der technischen Schutzmassnahmen</li><li>✓ Externe Audits</li></ul>



**Technische und organisatorische Massnahmen (TOM)**

**Security Incident Response Management**

Technische Massnahmen	Organisatorische Massnahmen
<ul style="list-style-type: none"> <li>✓ Einsatz von Firewall-Cluster, regelmässige Aktualisierung</li> <li>✓ Einsatz von Spamfilter, regelmässige Aktualisierung</li> <li>✓ Einsatz von Virens Scanner, regelmässige Aktualisierung</li> <li>✓ Regelmässige Aktualisierung von Betriebssystemen und Applikationen</li> </ul>	<ul style="list-style-type: none"> <li>✓ Prozess zur Erkennung und Meldung von Sicherheitsvorfällen</li> <li>✓ Dokumentierte Vorgehensweise im Umgang mit Datensicherheitsvorfällen</li> <li>✓ Einbindung des Datenschutzberaters (DSB)</li> <li>✓ Einbindung des Informationssicherheitsbeauftragten (CISO)</li> <li>✓ Dokumentation von Sicherheitsvorfällen</li> <li>✓ Prozess und Verantwortlichkeit zur Nachbesserung von Sicherheitsvorfällen</li> <li>✓ Cyber-Security Incident Management Konzept</li> </ul>

**Datenschutzfreundliche Voreinstellungen: Privacy by design / Privacy by default**

Technische Massnahmen	Organisatorische Massnahmen
<ul style="list-style-type: none"> <li>✓ Erhebung von Personendaten nur wenn erforderlich und mit Einwilligung</li> </ul>	<ul style="list-style-type: none"> <li>✓ Auskunftsrecht ist jederzeit gewährleistet</li> </ul>