

Technische und organisatorische Massnahmen (TOM)

Inhaltsverzeichnis

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



Technische und organisatorische Massnahmen (TOM)

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

Für alle Auftragsverarbeitungen gemäss Art. 9 DSG

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 Rechenzentrum

(Massnahmen zur Verhinderung von Zutritten Unberechtigter zu Datenverarbeitungsanlage)

Technische Massnahmen	Organisatorische Massnahmen
☑ Vereinzelungsanlagen	☑ Personenidentifikation
☑ Videoüberwachung	☑ Protokollierung der Zutritte
☑ elektronisches Schliesssystem mit Berechtigungsmanagement	☑ vertragliche Absicherung (NDA) mit Dienstleistern (Wartung)
☑ Alarmsystem	☑ Sorgfältige Auswahl von Personal und Lieferanten
☑ Sicherheitsschlösser	☑ Ausweise für Mitarbeitende und Gäste
	☑ Wachpersonal
	☑ Restriktive Zugangsrichtlinien
	☑ Besucherbegleitung ausschliesslich durch berechtigte Mitarbeitende



Technische und organisatorische Massnahmen (TOM)

Zugangskontrolle
(Massnahmen zur Verhinderung des Zugangs Unberechtigter zu Datenverarbeitungsanlage)

Technische Massnahmen	Organisatorische Massnahmen
☑ Personen-Authentifikation ☑ Zwei-Faktor Authentifizierung (2FA) ☑ Einsatz Firewall-Cluster ☑ Einsatz von VPN-Technologien	☑ Berechtigungskonzept ☑ regelmässige Überprüfung der Benutzerberechtigungen ☑ zentrales Passwort-Management ☑ Passwortrichtlinien ☑ Protokollierung von Zugriffen ☑ Richtlinie IT-Nutzung für Mitarbeitende ☑ Home-Office Weisung ☑ Umfassende Sensibilisierung und stetige Fortbildung der Mitarbeitenden im Bereich Cyber-Security und Datenschutz



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
☑ Protokollierung von Zugriffen ☑ Professionelle physische Vernichtung von Datenträgern	☑ Minimale Anzahl Administratoren ☑ Verwalten von Benutzerberechtigungen durch Administratoren ☑ Accounts der austretenden Mitarbeitenden werden umgehend deaktiviert Alle Administrationszugriffe werden protokolliert

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
☑ Physikalische und virtuelle Trennung (Systeme / Datenbanken / Storage) ☑ Trennung von Produktiv- und Testumgebung ☑ Mandantenfähigkeit relevanter Anwendungen	☑ Berechtigungs- und Zugriffskonzept ☑ Restriktives Berechtigungskonzept



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
☑ Verschlüsselte Übertragung der Daten ☑ Verschlüsselte Speicherung der Daten ☑ keine Weitergabe von pseudonymisierten Daten an Dritte	☑ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. Löschfristen gemäss AGB

Verfügbarkeits- und Belastbarkeitskontrolle

Technische Massnahmen	Organisatorische Massnahmen
☑ Unterbrechungsfreie Stromversorgung (USV) ☑ Schutz gegen Feuer, Rauch, Überflutungen, Feuchtigkeit etc. ☑ Klimaüberwachung der Server Räume ☑ Notstrom-Generator ☑ Redundante Stromversorgung ☑ Redundanter Storage ☑ Videoüberwachung ☑ Alarmanlage ☑ Monitoring-Systeme	☑ Backup-Konzept ☑ Business Continuity Management (BCM) ☑ Prüfung des Wiederherstellung-Prozesses ☑ Reglemässige Überprüfung und Tests der Notfallpläne ☑ Security Incident Management Weisung



Technische und organisatorische Massnahmen (TOM)

Regelmässige Überprüfung, Bewertung und Evaluierung	
Technische Massnahmen	**Organisatorische Massnahmen**
☑ Zugriff der Mitarbeitenden auf interne Weisungen	☑ Datenschutzberater DSB (extern) ☑ Informationssicherheitsbeauftragter CISO (extern) ☑ Schulung der Mitarbeitenden im Bereich Cyber-Security und Datenschutz ☑ Regelmässige Überprüfung der Wirksamkeit der technischen Schutzmassnahmen ☑ Externe Audits



Technische und organisatorische Massnahmen (TOM)

Security Incident Response Management

Technische Massnahmen	Organisatorische Massnahmen
☑ Einsatz von Firewall-Cluster, regelmässige Aktualisierung ☑ Einsatz von Spamfilter, regelmässige Aktualisierung ☑ Einsatz von Virenscanner, regelmässige Aktualisierung ☑ Regelmässige Aktualisierung von Betriebssystemen und Applikationen	☑ Prozess zur Erkennung und Meldung von Sicherheitsvorfällen ☑ Dokumentierte Vorgehensweise im Umgang mit Datensicherheitsvorfällen ☑ Einbindung des Datenschutzberaters (DSB) ☑ Einbindung des Informationssicherheits-beauftragten (CISO) ☑ Dokumentation von Sicherheitsvorfällen ☑ Prozess und Verantwortlichkeit zur Nachbesserung von Sicherheitsvorfällen ☑ Cyber-Security Incident Management Konzept

Datenschutzfreundliche Voreinstellungen: Privacy by design / Privacy by default

Technische Massnahmen	Organisatorische Massnahmen
☑ Erhebung von Personendaten nur wenn erforderlich und mit Einwilligung	☑ Auskunftsrecht ist jederzeit gewährleistet