

Anlage 2 zum Auftragsverarbeitungsvertrag: Technische und organisatorische Maßnahmen (TOMs) nach Artikel 32 DSGVO

Die technischen und organisatorischen Maßnahmen (TOMs) dienen dazu, ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten und insbesondere die Rechte und Freiheiten betroffener Personen zu schützen. Im Folgenden stellen wir die von uns implementierten TOMs vor.

Detailliertere Informationen zu einzelnen Maßnahmen finden Sie unter:
<https://docs.hetzner.com/de/general/others/technical-and-organizational-measures>.

1 Zutrittskontrolle

Die Zutrittskontrolle regelt, wer physischen Zugang zu einem Gelände, Gebäude oder Raum erhält.

Maßnahme	Rechenzentrumstandorte	Verwaltungsgebäude
Elektronisches Zutrittskontrollsystem mit Protokollierung	✓	✓
Dokumentierte Vergabe von Zutrittsmedien	✓	✓
Flächendeckende Videoüberwachung	✓	✓
Richtlinie zum Besuchermanagement	✓	✓
Hochsicherheitszaun mit Übersteig- und Untergrabenschutz um den gesamten Datacenter-Park	✓	Nicht zutreffend
Separierte Colocation-Bereiche mit abschließbaren Racks	✓	Nicht zutreffend

Bitte beachten Sie für die nachstehenden Kapitel den folgenden Hinweis:

Bei unseren **dedizierten Servern / Cloud Servern** liegt die Verantwortung für die Verwaltung, Wartung und Sicherheit der Serverinfrastruktur vollständig beim Auftraggeber.

Bei unseren **Managed-Produkten** übernehmen wir die Verantwortung für die Wartung, Administration und Sicherheit Ihrer Systeme.

2 Zugangskontrolle

Die Zugangskontrolle definiert, wer sich auf einem System einloggen darf, sodass nur autorisierte Personen Zugriff auf dieses erhalten.

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
Eigenes Kundenkonto mit zahlreichen Verwaltungsoptionen und Zugang zur Administrationsoberfläche	✓	✓	✓	✓	✓	✓	✓	✓
Nachvollziehbare Protokollierung von Zugriffs- und Änderungsvorgängen im Kundenaccount	✓	✓	✓	✓	✓	✓	✓	✓
Passwortpflicht für das Kundenkonto mit festgelegten Mindestanforderungen	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
Option zur Zwei-Faktor-Authentifizierung (2FA) für Kundenkonto	✓	✓	✓	✓	✓	✓	✓	✓
Serverzugriff erfolgt ausschließlich durch Auftraggeber	✓	✓	✓	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)
Administrativer Zugriff erfolgt ausschließlich durch autorisierte Hetzner-Mitarbeitende im Rahmen der vereinbarten Leistung über mehrstufige Authentifizierung und kryptografischem Schutz je nach Produkt von reiner Infrastrukturwartung bis hin zu vollständiger Serververwaltung	Nicht zutreffend (siehe vorherige Zeile)	Nicht zutreffend (siehe vorherige Zeile)	Nicht zutreffend (siehe vorherige Zeile)	✓	✓	✓	✓	✓
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	✓	✓

3 Zugriffskontrolle

Die Zugriffskontrolle regelt, welche Berechtigungen eine Person innerhalb eines Systems hat. Sie bestimmt, was ein Benutzer nach erfolgreichem Zugang sehen, ändern oder ausführen darf.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Regelmäßige Sicherheitsupdates	Obliegt Auftraggeber	Obliegt Auftraggeber	✓ für zugrunde liegende Cloud-Infrastruktur	✓ für zugrunde liegende Infrastruktur	✓	✓	✓	✓
Revisionssicheres, verbindliches Berechtigungsverfahren auf Basis eines Rollen- und Berechtigungskonzeptes	Obliegt Auftraggeber	Obliegt Auftraggeber	✓ Für Zugriffe auf Cloud-Infrastruktur Für virtuellen Server ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich
Pflege, Sicherheit und Aktualität der übertragenen Daten/Software	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓ bzgl. Zugriffe auf Cloud-Server	✓	✓	✓	✓	✓

4 Datenträgerkontrolle

Die Datenträgerkontrolle umfasst Maßnahmen und Verfahren, die sicherstellen, dass die Nutzung, der Zugriff und der Transport von physischen Datenträgern kontrolliert und vor unbefugtem Zugriff geschützt werden.

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
Definiertes Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung je nach Produktart unterschiedlich umgesetzt	Obliegt Auftraggeber	✓	✓	✓	✓	✓	✓	✓
Physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung	Obliegt Auftraggeber	✓	✓	✓	✓	✓	✓	✓
Physischer Zugriff auf Datenträger nur in definierten Bereichen; Transport standortübergreifend ausschließlich in verschlossenen Transportboxen	Obliegt Auftraggeber	✓	✓	✓	✓	✓	✓	✓

5 Trennungskontrolle

Maßnahmen zur Trennungskontrolle stellen sicher, dass Daten unterschiedlicher Kunden oder Anwendungen innerhalb eines Systems klar voneinander getrennt verarbeitet und gespeichert werden.

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
Physische oder logische Trennung von Daten	Obliegt Auftraggeber	Obliegt Auftraggeber	✓	✓	✓	✓	✓	✓
Physische und logische Trennung von Backup-Daten	Obliegt Auftraggeber	Obliegt Auftraggeber	✓	✓	✓	✓	Nicht zutreffend	Obliegt Auftraggeber
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	Nicht zutreffend	Nicht zutreffend

6 Pseudonymisierung

Durch Maßnahmen zur Pseudonymisierung werden personenbezogene Daten so modifiziert, dass sie nur unter Verwendung von Zusatzinformationen einer bestimmten Person zugeordnet werden können.

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
Pseudonymisierung der auf den Systemen gespei- cherten Daten	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber

7 Vertraulichkeit

Maßnahmen zur Vertraulichkeit stellen sicher, dass personenbezogene Daten bei der Verarbeitung und Speicherung vor unberechtigtem Zugriff oder Weitergabe geschützt werden.

Maßnahme	Umsetzung
Verpflichtungserklärung der Hetzner-Mitarbeitenden vor Tätigkeitsbeginn zur datenschutzkonformen Verarbeitung personenbezogener Daten	✓
Verpflichtungserklärung externer Personen vor Tätigkeitsbeginn zu Verschwiegenheit und Umsetzung von TOMs (bei Bedarf)	✓
Regelmäßige Sensibilisierungen und Schulungen der Hetzner-Mitarbeitenden bzgl. Datenschutz- und Informationssicherheitsthemen	✓
Verschlüsselungsoptionen für die Datenübertragung je nach Produktart unterschiedlich umgesetzt	✓
Verschlüsselung der Daten (at rest)	Obliegt Auftraggeber
Verschlüsselung des Backups (at rest)	Obliegt Auftraggeber Ausnahme bei Managed-Servern: ✓

8 Integrität

Die Integrität stellt sicher, dass Daten und Systeme vollständig, unverfälscht und korrekt bleiben – sowohl bei der Speicherung als auch bei der Übertragung.

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
Protokollierung von Da- tenänderungen	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber	✓	✓	✓	✓	✓
Verantwortung für Ein- gabe und Bearbeitung von Daten	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber
Virens Scanner / Sicher- heitsprüfung	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	✓	✓	Rootkit- Prüfungen	Rootkit- Prüfungen	-
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	✓	✓

9 Verfügbarkeit, Belastbarkeit und Netzwerksicherheit

Die Verfügbarkeit fokussiert sich auf die kontinuierliche Funktionsfähigkeit eines Systems. Die Belastbarkeit sorgt in diesem Zusammenhang dafür, dass die Verfügbarkeit auch unter außergewöhnlichen Umständen gewährleistet bleibt. Die Netzwerksicherheit umfasst Maßnahmen zum Schutz der Netzwerkinfrastruktur vor unbefugten Zugriffen und Angriffen.

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
<u>Betrieb und Support</u>								
24/7 technischer Support direkt im Rechenzentrum	Nicht zutreffend Remote Hands auf An- frage	✓	✓	✓	✓	✓	✓	✓
Eskalationskette für Stö- rungen und Notfälle	siehe Produktbeschreibung							
Monitoring	Obliegt Auftragge- ber	Obliegt Auftragge- ber	✓ für Host Für virtuellen Server ist Auf- traggeber selbst verant- wortlich	✓	✓	✓	✓	✓

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
<u>Stromversorgung, Klimatisierung und Gebäudetechnik</u>								
Unterbrechungsfreie Stromversorgung durch redundante USVs und NEA	✓	✓	✓	✓	✓	✓	✓	✓
Redundante Stromein- speisung vom Umspann- werk	✓	✓	✓	✓	✓	✓	✓	✓
Redundante und energie- effiziente Kühlung durch direkte freie Kühlung und Klimaanlagen	✓	✓	✓	✓	✓	✓	✓	✓
Kaltgangeinhausung in überdurchschnittlich ho- hem Doppelboden	✓	✓	✓	✓	✓	✓	✓	✓
Überwachung der pro- zessrelevanten Größen über intelligentes Mess-, Steuer-, Regel- und Über- wachungssystem	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
<u>Brandschutz</u>								
Flächendeckende Brand- früherkennungsmechanis- men mit automatischer Alarmierung und Leitstel- lenanbindung	✓	✓	✓	✓	✓	✓	✓	✓
Dynamisches Brand- schutzkonzept	✓	✓	✓	✓	✓	✓	✓	✓
Regelmäßige Schulungen und Notfallübungen der Brandschutzhelfer	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
<u>Netzwerk und Angriffsschutz</u>								
Redundante und hochverfügbare Netzwerkinfrastruktur 99,9 %ige Netzwerkverfügbarkeit gemäß AGB	✓	✓	✓	✓	✓	✓	✓	✓
Dauerhaft aktive DDoS-Erkennung	✓	✓	✓	✓	✓	✓	✓	✓
Einsatz von Firewall und Portreglementierungen	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	✓	✓	✓	✓	✓
Individuell konfigurierbare Firewall	Nicht zutreffend	✓	✓	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	✓
Providerverwaltete Firewall mit 24/7-Monitoring	Nicht zutreffend	Nicht zutreffend (siehe vorherige Zeile)	Nicht zutreffend (siehe vorherige Zeile)	✓	✓	✓	✓	Nicht zutreffend (siehe vorherige Zeile)

Maßnahme	Colo- cation	Dedicated Server	Cloud Server	Managed Server	Web- hosting	Storage Share	Storage Box	Object Storage
<u>Backup und Systemschutz</u>								
Backup- und Recovery- Konzept	Obliegt Auftrag- geber	Obliegt Auftrag- geber	Obliegt Auftrag- geber Backup/Snap- shot können kostenpflichtig hinzugebucht werden	✓ zum Teil ab- hängig von gebuchten Leistungen	✓	✓ eigenes Ba- ckup empfoh- len	Obliegt Auftrag- geber Snapshots, abhängig von gebuchter Leistung	Obliegt Auftrag- geber Redundante Speicherung innerhalb des Clustersys- tems
Festplattenspiegelung	Obliegt Auftragge- ber	Obliegt Auftragge- ber	Obliegt Auftragge- ber	✓	✓	✓	✓	✓

10 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Regelmäßige Überprüfungs-, Bewertungs- und Evaluierungsverfahren gewährleisten die kontinuierliche Einhaltung und Verbesserung von Datenschutz- und Sicherheitsstandards.

Maßnahme	Umsetzung
Datenschutz- und Informationssicherheits-Management-System (DMS, ISMS)	✓
Bestellung eines Datenschutz- und Informationssicherheitsbeauftragten und Einbindung dieser in betriebliche Prozesse	✓
Datenschutzfreundliche Voreinstellungen bei Softwareentwicklungen (Privacy by default und Privacy by design)	✓
Incident-Response-Management	✓
Zertifizierungen nach ISO 27001, § 8a BSI-KritisV und BSI C5 Typ 2 Testat	✓
Jährliche Überprüfung der TOMs durch externen Dienstleister	✓
Jährliche Überprüfung der ordnungsgemäßen Verbindungspreisberechnung über Sachverständigengutachten gemäß § 63 TKG	✓
EMAS-Zertifizierung (ISO 14001) des Umweltmanagementsystem der deutschen Standorte	✓