TÜVRheinland®
Genau. Richtig.

Bericht

- Vertraulich -

Prüfung der technischen und organisatorischen Maßnahmen der Rechenzentren

bei der

HETZNER

Hetzner Online GmbH

Version 1.0

Bericht Nr. 63017020-01

Köln, den 11. Februar 2025

TÜV Rheinland i-sec GmbH

Allgemeine Informationen zur durchgeführten Untersuchung

Auftraggeber:	Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen
Beauftragtes Institut:	**TÜV Rheinland i-sec GmbH** Am Grauen Stein | 51105 Köln Freigerichter Straße 1-3 | 63571 Gelnhausen Dudweilerstraße 17 | 66111 Saarbrücken Zeppelinstr. 1 | 85399 Hallbergmoos Köln HRB 30644 | USt.-ID-Nr: DE812864532 Tel.: +49 221-806 0 / Fax 0221-806 2295 E-Mail: service@i-sec.tuv.com
Untersuchungsumfang:	Prüfung der technischen und organisatorischen Maßnahmen der Rechenzentren an den Standorten: • Helsinki (Tuusula, Finnland) (Letzte Ortsbegehung am 01.03.2023) • Nürnberg (Letzte Ortsbegehung am 07.02.2024) • Falkenstein (Vogtl.) (Letzte Ortsbegehung am 11.02.2025)
Mitgeltende Unterlagen:	Auftragsdatenverarbeitungsvertrag inkl. Anlage 2: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO der Hetzner Online GmbH
Projektleiter:	Bernd Zimmer

Inhaltsverzeichnis

1 Zusammenfassung

Die TÜV Rheinland i-sec GmbH bestätigt der Hetzner Online GmbH die Einhaltung der, den Kunden bereitgestellten, Informationen zu den getroffenen technischen und organisatorischen Maßnahmen gemäß Art. 28 DS-GVO. Die Prüfung basierte auf den allgemein zugänglichen technischen und organisatorischen Maßnahmen, die zum Zeitpunkt des Audits unter https://www.hetzner.com/AV/TOM.pdf aufrufbar waren. Die vorgenannten technischen und organisatorischen Maßnahmen sind Bestandteil des Auftragsverarbeitungsvertrages zwischen der Hetzner Online GmbH (Auftragnehmer) und dem Kunden (Auftraggeber).

Bei der Prüfung wurden keine Abweichungen festgestellt.

2 Grundlagen und Methodik

Dieser Abschnitt beschreibt Ausgangssituation, Geltungsbereich, Zielsetzung und Prüf- und Bewertungsgrundlagen der durchgeführten Untersuchung.

2.1 Ausgangssituation und Zielsetzung

Die Firma Hetzner Online GmbH ist am Markt im Bereich des Hostings bzw. des Housings als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO tätig. Im Rahmen dieser Tätigkeit werden DS-GVO-konforme Auftragsverarbeitungsverträge mit den Kunden abgeschlossen. Die Verträge beinhalten (gemäß Art. 28 Abs. 3 lit. e DS-GVO) technische und organisatorische Maßnahmen, die Gegenstand dieser Prüfung sind.

Seit Oktober 2016 ist die Hetzner Online GmbH nach dem internationalen Standard ISO/IEC 27001:2013 zertifiziert. Die Zertifizierung ist bis September 2025 gültig und umfasst alle Standorte in Deutschland und Finnland. Als Geltungsbereich des Zertifikats ist genannt:

„Der Anwendungsbereich des Informationssicherheitsmanagementsystems umfasst alle Hosting-Dienstleistungen und die Rechenzentren der Hetzner Online GmbH.“

Das aktuelle Zertifikat ist auf der Website der Hetzner Online GmbH abrufbar unter: https://www.hetzner.com/de/unternehmen/zertifizierung/.

2.2 Geltungsbereich

Datacenter-Parks an den Standorten:

- Helsinki/Tuusula (Finnland)
- Nürnberg
- Falkenstein/Vogtland

2.3 Prüf-/Audit-Grundlage

Als Prüfgrundlagen wurden verwendet:

- Technische und organisatorischen Maßnahmen der Firma Hetzner Online GmbH, die unter dem Link https://www.hetzner.com/AV/TOM.pdf abrufbar sind.
- EU-Datenschutz-Grundverordnung (EU DS-GVO)

2.4 Vorgehensweise

Im Rahmen einer Ortsbegehung wurden die technischen und organisatorischen Maßnahmen an den Standorten zum jeweiligen Prüfdatum nachvollzogen und die Konformität mit den Angaben der Hetzner Online GmbH überprüft.

Neben der Ortsbegehung wurden Interviews mit den beteiligten Mitarbeitern durchgeführt und die getroffenen Maßnahmen mit den beschriebenen, respektive mit Kunden vertraglich vereinbarten Maßnahmen, verglichen und bewertet.

Folgende Personen wurden beim Audit befragt:

Simon Beißer	IT Sicherheitsbeauftragter
Alena Scholz	Datenschutzbeauftragte

3 Ergebnis der Prüfung

Die von der Hetzner Online GmbH gemachten Angaben in der „*Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage*“ sind implementiert und entsprechen den vertraglich zugesicherten Maßnahmen.

4 Ergebnisse im Detail

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

I. Zutrittskontrolle

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

Maßnahme	Rechenzentrumsstandorte	Verwaltungsgebäude
Elektronisches Zutrittskontrollsystem mit Protokollierung	✓	✓
Dokumentierte Vergabe von Zutrittsmedien	✓	✓
Flächendeckende Videoüberwachung	✓	✓
Richtlinie zum Besuchermanagement	✓	✓
Hochsicherheitszaun mit Übersteigschutz 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** 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.

II. Zugangskontrolle

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

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Eigenes Kundenkonto mit zahlreichen Verwaltungs-optionen und Zugang zur Administrationsoberflä-che	✓	✓	✓	✓	✓	✓	✓	✓
Nachvollziehbare Proto-kollierung von Zugriffs- und Änderungsvorgän-gen im Kundenaccount	✓	✓	✓	✓	✓	✓	✓	✓
Passwortpflicht für das Kundenkonto mit festge-legten Mindestanforde-rungen	✓	✓	✓	✓	✓	✓	✓	✓
Option zur Zwei-Faktor-Authentifizierung (2FA) für Kundenkonto	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Serverzugriff erfolgt ausschließlich durch Auftraggeber	✓	✓	✓	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
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	Nicht zutreffend	Nicht zutreffend	✓	✓	✓	✓	Nicht zutreffend
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)
Virenscanner / Sicherheitsprüfung	Obliegt Auftraggeber	✓	✓	✓	✓	Rootkit-Prüfungen	Rootkit-Prüfungen	-
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	✓

III. 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	Colocation	Dedicated Server	Cloud Server	Managed Server	Webhosting	Storage Share	Storage Box	Object Storage	Interne Verwaltungssysteme
Regelmäßige Sicherheitsupdates	Obliegt Auftraggeber	Obliegt Auftraggeber	✓ für zugrunde liegende Cloud-Infrastruktur	✓	✓	✓	✓	✓	✓
Revisionssicheres, verbindliches Berechtigungsverfahren auf Basis eines Rollen- und Berechtigungskonzeptes	Obliegt Auftraggeber	Obliegt Auftraggeber	✓ Es erfolgen Zugriffe auf die Cloud-Infrastruktur	✓	✓	✓	✓	✓	✓
Pflege, Sicherheit und Aktualität der übertragenen Daten/Software	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	NA
(Zusätzliche) Maßnahmen obliegen Auftraggeber	✓	✓	✓ bzgl. Zugriffe auf Cloud-Server	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

IV. 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	Interne Verwal-tungs-systeme
Definiertes Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung je nach Produktart unterschiedlich umgesetzt	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓	✓	✓
Physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓	✓	✓

V. 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	Interne Verwal-tungs-systeme
Physische oder logische Tren-nung von Daten	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓	✓
Physische und lo-gische Trennung von Backup-Daten	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	Nicht zu-treffend	✓
(Zusätzliche) Maßnahmen ob-liegen Auftragge-ber	✓	✓	✓	Nicht zu-treffend	Nicht zu-treffend	Nicht zu-treffend	Nicht zu-treffend	Nicht zu-treffend	Nicht zutreffend

VI. 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
Für die Pseudonymisierung ist der Auftraggeber verantwortlich	✓	✓	✓	✓	✓	✓	✓	✓

VII. Vertraulichkeit

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

Maßnahme	Allgemein	Produkt-abhängig
Verpflichtungserklärung der Hetzner-Mitarbeitenden vor Tätigkeitsbeginn zur datenschutzkonformen Verarbeitung personenbezogener Daten	✓	-
Regelmäßige Sensibilisierungen und Schulungen der Hetzner-Mitarbeitenden bzgl. Datenschutz- und Informationssicherheitsthemen	✓	-
Verschlüsselungsoptionen für die Datenübertragung	-	✓

VIII. 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	Interne Verwal-tungs-systeme
Protokollierung von Datenänderungen	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓
Verantwortung für Eingabe und Bear-beitung von Daten obliegt Auftragge-ber	✓	✓	✓	✓	✓	✓	✓	✓	✓ Kunde kann Kundenda-tenänderung über Kun-denaccount selbstständig vornehmen
(Zusätzliche) Maß-nahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	✓	✓	Nicht zu-treffend

IX. Verfügbarkeit und Belastbarkeit

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.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage	Interne Verwal-tungs-systeme
24/7 technischer Support direkt im Rechenzentrum	Nicht zu-treffend	✓	✓	✓	✓	✓	✓	✓	✓
Unterbrechungs-freie Stromversor-gung durch redun-dante USVs und NEA	✓	✓	✓	✓	✓	✓	✓	✓	✓
Redundante und hochverfügbare Netzwerkinfrastruk-tur	✓	✓	✓	✓	✓	✓	✓	✓	✓
Flächendeckende Brandfrüherken-nungsmechanis-men mit automati-scher Alarmierung und Leitstellenan-bindung	✓	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage	Interne Verwal-tungs-systeme
Dynamisches Brandschutzkon-zept	✓	✓	✓	✓	✓	✓	✓	✓	✓
Regelmäßige Schu-lungen und Notfal-lübungen der Brandschutzhelfer	✓	✓	✓	✓	✓	✓	✓	✓	✓
Redundante und energieeffiziente Kühlung durch di-rekte freie Kühlung und Klimaanlagen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kaltgangeinhau-sung	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kontinuierliche Temperaturüber-wachung in Server-räumen und Verteil-erschränken	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dauerhaft aktive DDoS-Erkennung	✓	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage	Interne Verwal-tungs-systeme
Backup- und Re-covery-Konzept	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓ abhängig von gebuchten Leistungen	✓ zum Teil ab-hängig von gebuchten Leistungen	Einzelne Datei-wiederher-stellung möglich	RAID-basiertes Speicher-backend	Snapshots, abhängig von ge-buchter Leistung	Redun-dante Speiche-rung in-nerhalb des Clus-tersystems	✓ tägliche Si-cherung aller relevanten Daten
Festplatten-spieglung	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓ bei allen rele-vanten Ser-vern
Monitoring	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓ bei allen rele-vanten Ser-vern
Eskalationskette für Störungen und Notfälle	siehe Produktbeschreibung								✓
Einsatz von Soft-warefirewall und Portreglementie-rungen	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓

X. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

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

Maßnahme	Allgemein	Produkt-abhängig
Datenschutz-Informationssicherheits-Management-System (DIMS)	✓	-
Incident-Response-Management	✓	-
Datenschutzfreundliche Voreinstellungen bei Softwareentwicklungen (Privacy by default)	✓	-
Bestellung eines Datenschutz- und Informationssicherheitsbeauftragten und Einbindung dieser in betriebliche Prozesse	✓	-

5 Allgemeine Hinweise

Im Hinblick auf den Stichprobencharakter der Untersuchung ist darauf hinzuweisen, dass außerhalb der im Zusammenhang mit dieser Untersuchung abgeprüften Aspekte weitere Stärken, aber auch potenzielle Risiken vorhanden sein können.

Obwohl die Durchführung der Prüfung größtmöglicher Sorgfalt unterlag, schließt die TÜV Rheinland i-sec GmbH daher Haftung für vorhandene und nicht erkannte potenzielle Risiken aus.

Das Prüfergebnis entbindet das Unternehmen in keiner Weise von der Weiterverfolgung seiner Sicherheitsziele.

Das Unternehmen ist in jedem Fall für seine Maßnahmen zur Sicherstellung seiner Sicherheitsziele selbst verantwortlich.

Jede Haftung für eventuelle Schäden, die aus einer falschen Anwendung der hier gegebenen Informationen resultieren, wird ausgeschlossen.