TÜVRheinland®
Genau. Richtig.

Bericht

- Vertraulich -

Prüfung der technischen und organisatorischen Maßnahmen der Rechenzentren

bei der

HETZNER

Hetzner Online GmbH

Version 1.0

Bericht Nr. 63017991-01

Köln, den 19. Februar 2026

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 19.02.2026) • 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 zertifiziert. Die Zertifizierung ist bis September 2028 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."

Zudem hält die Hetzner Online GmbH seit Dezember 2025 ein BSI C5 Typ 2 Testat.

Die weiteren Informationen zu den Zertifizierungen finden Sie unter: https://docs.hetzner.com/de/general/company-and-policy/information-security-at-hetzner/

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:

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 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** 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 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 Verwaltungs-optionen und Zugang zur Administrationsoberflä-che	✓	✓	✓	✓	✓	✓	✓	✓
Nachvollziehbare Proto-kollierung von Zugriffs- und Änderungsvorgängen im Kundenaccount	✓	✓	✓	✓	✓	✓	✓	✓
Passwortpflicht für das Kundenkonto mit festge-legten Mindestanforde-rungen	✓	✓	✓	✓	✓	✓	✓	✓

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	✓	✓	✓	✓	✓	✓	✓	✓

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	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Regelmäßige Sicherheitsupdates	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓ für zugrunde liegende Cloud-Infra-struktur	✓ für zugrunde liegende Infra-struktur	✓	✓	✓	✓
Revisionssicheres, verbindliches Berechtigungs-verfahren auf Basis eines Rollen- und Berechtigungskonzeptes	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓ 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 Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓ bzgl. Zugriffe auf Cloud-Server	✓	✓	✓	✓	✓

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
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	✓	✓	✓	✓	✓	✓	✓
Physischer Zugriff auf Datenträger nur in definierten Bereichen; Transport standortübergreifend ausschließlich in verschlossenen Transportboxen	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
Physische oder logische Trennung von Daten	Obliegt Auftragge-ber	Obliegt Auftragge-ber	✓	✓	✓	✓	✓	✓
Physische und logische Trennung von Backup-Da-ten	Obliegt Auftragge-ber	Obliegt Auftragge-ber	✓	✓	✓	✓	Nicht zutreffend	Obliegt Auftragge-ber
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	Nicht zutreffend	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	Colocation	Dedicated Server	Cloud Server	Managed Server	Webhosting	Storage Share	Storage Box	Object Storage
Pseudonymisierung der auf den Systemen gespeicherten Daten	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber	Obliegt Auftraggeber

VII. 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: ✓

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
Protokollierung von Datenänderungen	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓
Verantwortung für Eingabe 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
Virenscanner / Sicherheitsprüfung	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	✓	✓	Rootkit-Prüfungen	Rootkit-Prüfungen	-
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	✓	✓

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. 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
Betrieb und Support								
24/7 technischer Support direkt im Rechenzentrum	Nicht zutreffend Remote Hands auf Anfrage	✓	✓	✓	✓	✓	✓	✓
Eskalationskette für Störungen und Notfälle	siehe Produktbeschreibung							
Monitoring	Obliegt Auftraggeber	Obliegt Auftraggeber	✓ für Host Für virtuellen Server ist Auftraggeber selbst verantwortlich	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Stromversorgung, Klimatisierung und Gebäudetechnik								
Unterbrechungsfreie Stromversorgung durch redundante USVs und NEA	✓	✓	✓	✓	✓	✓	✓	✓
Redundante Stromeinspeisung vom Umspannwerk	✓	✓	✓	✓	✓	✓	✓	✓
Redundante und energieeffiziente Kühlung durch direkte freie Kühlung und Klimaanlagen	✓	✓	✓	✓	✓	✓	✓	✓
Kaltgangeinhausung in überdurchschnittlich hohem Doppelboden	✓	✓	✓	✓	✓	✓	✓	✓
Überwachung der prozessrelevanten Größen über intelligentes Mess-, Steuer-, Regel- und Überwachungssystem	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Brandschutz								
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
Netzwerk und Angriffsschutz								
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
Backup und Systemschutz								
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
Festplattenspieglung	Obliegt Auftragge-ber	Obliegt Auftragge-ber	Obliegt Auftragge-ber	✓	✓	✓	✓	✓

X. 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	✓

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.