TÜVRheinland®
Genau. Richtig.

Report

- Confidential -

Review of the technical and organizational measures of the data centers

at the

HETZNER

Hetzner Online GmbH

Version 1.0

Report no. 63017991-01

Cologne,19. February 2026

TÜV Rheinland i-sec GmbH

General information on the examination carried out

Client:	Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen
Authorised institute:	**TÜV Rheinland i-sec GmbH** Am Grauen Stein | 51105 Cologne Freigerichter Straße 1-3 | 63571 Gelnhausen Dudweilerstraße 17 | 66111 Saarbrücken Zeppelinstr. 1 | 85399 Hallbergmoos Cologne HRB 30644 | VAT ID no.: DE812864532 Phone: +49 221-806 0 / Fax 0221-806 2295 E-mail: service@i-sec.tuv.com
Scope of investigation:	Checking the technical and organisational measures of the data centres at the locations: • Helsinki (Tuusula, Finland) (Last site visit on 19/02/2026) • Nuremberg (last site inspection on 07/02/2024) • Falkenstein (Vogtl.) (Last site inspection on 11/02/2025)
Other applicable documents:	Contract data processing agreement incl. Annex 2: Technical and organisational measures in accordance with Art. 32 GDPR of Hetzner Online GmbH
Project manager:	Bernd Zimmer

Table of contents

1 Summary

TÜV Rheinland i-sec GmbH confirms Hetzner Online GmbH's compliance with the information provided to customers on the technical and organisational measures taken in accordance with Art. 28 GDPR. The audit was based on the generally accessible technical and organisational measures that were available at https://www.hetzner.com/AV/TOM.pdf at the time of the audit. The aforementioned technical and organisational measures are part of the order processing contract between Hetzner Online GmbH (contractor) and the customer (client).

No deviations were identified during the audit.

2 Basics and methodology

This section describes the initial situation, scope, objectives and testing and assessment principles of the study carried out.

2.1 Initial situation and objectives

Hetzner Online GmbH is active on the market in the field of hosting or housing as a processor within the meaning of Art. 28 GDPR. As part of this activity, GDPR-compliant order processing contracts are concluded with customers. The contracts contain technical and organisational measures (in accordance with Art. 28 para. 3 lit. e GDPR), which are the subject of this audit.

Since October 2016, Hetzner Online GmbH has been certified according to the international standard ISO/IEC 27001 certified. The certification is valid until September 2028 and covers all locations in Germany and Finland. The scope of the certificate is as follows:

"The scope of the information security management system includes all hosting services and the data centres."

In addition, Hetzner Online GmbH has held a BSI C5 Type 2 certificate since December 2025.

Further information about the certifications can be found at:

https://docs.hetzner.com/general/company-and-policy/information-security-at-hetzner/

2.2 Scope of application

Data centre parks at the locations:

- Helsinki/Tuusula (Finland)
- Nuremberg (Germany)
- Falkenstein/Vogtland (Germany)

2.3 Test/audit basis

The following were used as test bases:

- Technical and organisational measures of Hetzner Online GmbH, which are available at the link https://www.hetzner.com/AV/TOM.pdf.
- EU General Data Protection Regulation (EU GDPR)

2.4 Procedure

During an on-site inspection, the technical and organisational measures at the locations were verified on the respective inspection date and conformity with the information provided by Hetzner Online GmbH was checked.

In addition to the site inspection, interviews were conducted with the employees involved and the measures taken were compared and evaluated with the measures described or contractually agreed with customers

The following persons were interviewed during the audit:

Alena Scholz Data Protection Officer

3 Result of the audit

The information provided by Hetzner Online GmbH in "*Annex 2 to the contract pursuant to Art. 28 GDPR: Technical and organisational measures in accordance with Art. 32 GDPR and Annex*" have been implemented and correspond to the contractually assured measures.

4 Results in detail

You can find more detailed information on individual measures at: https://docs.hetzner.com/general/others/technical-and-organizational-measures.

I. Access control

Physical access control defines who has physical access to a site, building, or room.

Measure	Data centers	Admin buildings
Electronic access control system with logging	✓	✓
Documented distribution of access media	✓	✓
Comprehensive video monitoring	✓	✓
Policy about how to handle visitors	✓	✓
High security perimeter fencing (with anti-climbing and anti-tunnelling protection) around the entire data center park	✓	NA
Separate colocation area with lockable racks	✓	NA

Please note the following information for the following chapters:
With our **dedicated servers**, the responsibility for the administration, maintenance and security of the server infrastructure lies entirely with the client.
With our **managed products**, we take responsibility for the maintenance, administration and security of your systems.

II. Electronic access control

The electronic access control defines who is allowed to log on to a system so that only authorized people have access to it.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Individual customer accounts with numerous management options and access to the administration interface	✓	✓	✓	✓	✓	✓	✓	✓
Traceable access logs and change logs for customer accounts	✓	✓	✓	✓	✓	✓	✓	✓
Required passwords for customer accounts with defined minimum requirements	✓	✓	✓	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Option for two-factor authentication (2FA) for customer accounts	✓	✓	✓	✓	✓	✓	✓	✓
Client has exclusive access to server	✓	✓	✓	NA (see next line)	NA (see next line)	NA (see next line)	NA (see next line)	NA (see next line)
Only authorized Hetzner employees have administrative access, within the scope of the agreed service; via multi-level authentication and cryptographic protection **Access done for tasks ranging from infrastructure maintenance to complete server management depending on product**	NA (see last line)	NA (see last line)	NA (see last line)	✓	✓	✓	✓	✓
Additional measures the responsibility of the Client	✓	✓	✓	✓	✓	✓	✓	✓

III. Internal access control

Internal access control defines which authorizations people have within a system. It defines what a user may see, change, or execute after accessing a system.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Regular updates	Client's responsibility	Client's responsibility	✓ for the underlying cloud infrastructure	✓ for the underlying infrastructure	✓	✓	✓	✓
Audit-proof, binding authorization procedure based on a role and authorization policy	Client's responsibility	Client's responsibility	✓ the cloud infrastructure is accessed client's responsibility for virtual machine	✓ client's responsibility for file access	✓ client's responsibility for file access	✓ client's responsibility for file access	✓ client's responsibility for file access	✓ client's responsibility for file access
Maintaining, securing, and updating transferred data/software	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility
Additional measures the responsibility of the Client	✓	✓	✓ regarding access to cloud servers	✓	✓	✓	✓	✓

IV. Transfer control

Transfer control includes measures and procedures that make sure that the use, access, and transport of physical data storage media are monitored and protected against unauthorized access.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Defined process for deleting data from storage drives after contract is complete **Implemented differently depending on product type**	Client's responsibility	✓	✓	✓	✓	✓	✓	✓
Storage drives are physically destroyed if data cannot be successfully erased	Client's responsibility	✓	✓	✓	✓	✓	✓	✓
Physical access to storage devices only in defined areas; transport across locations exclusively in locked transport boxes	Client's responsibility	✓	✓	✓	✓	✓	✓	✓

V. Isolation control

Measures for isolation control make sure that data for each different customer or application within a system is separated from each other when they are processed and stored.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Physical and logical separation of data	Client's responsibility	Client's responsibility	✓	✓	✓	✓	✓	✓
Physical and logical separation of back-up data	Client's responsibility	Client's responsibility	✓	✓	✓	✓	✓	NA
Additional measures the responsibility of the Client	✓	✓	✓	✓	✓	✓	NA	NA

VI. Pseudonymisation

Using pseudonymization methods, personal data is modified in such a way that it cannot be tied to specific people without additional information being provided.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Pseudonymization of data stored within the systems	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility

VII. Confidentiality

Confidentiality measures make sure that personal data is protected from unauthorized access or disclosure while it is being processed and stored.

Measure	Implementation
Hetzner employees sign a confidentiality agreement before they begin doing any work with personal data in compliance with data protection regulations	✓
Confidentiality agreement and implementation of TOMs by external persons before starting their activities for Hetzner (if necessary)	✓
Hetzner employees regularly get training to raise awareness for and knowledge about data protection and information security	✓
Encryption options for data transfers **(Implemented differently depending on product type)**	✓
Encryption of Data (at rest)	Client's responsibility
Encryption of Backups (at rest)	Client's responsibility Exception Managed Servers: ✓

VIII. Integrity

Data integrity measures make sure that data and systems remain complete, uncorrupted, and correct while they are being stored or transferred.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Data changes are logged in an audit-proof manner	Client's responsibility	Client's responsibility	Client's responsibility	✓	✓	✓	✓	✓
Responsibility for entering and processing data	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility	Client's responsibility
Virus scanner / Security tests	Client's responsibility	Client's responsibility	Client's responsibility	✓	✓	Rootkit tests	Rootkit tests	-
Additional measures the responsibility of the Client	✓	✓	✓	✓	✓	✓	✓	✓

IX. Availability and resilience

Availability measures focus on keeping the systems in continued working order. Resilience measures make sure that the data remains available even under exceptional circumstances. Network security includes measures to protect the network infrastructure from unauthorized access and attacks.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Operation and support								
24/7 technical support directly in data center	NA Remote hands on request	✓	✓	✓	✓	✓	✓	✓
Escalation chain for disruptions and emergencies	See product description							
Monitoring	Client's responsibility	Client's responsibility	✓ for Host Client's responsibility for virtual machine	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Power supply, climatization and facility management								
Uninterruptible power supply using redundant UPSs and emergency power supply system	✓	✓	✓	✓	✓	✓	✓	✓
Redundant power supply from the substation	✓	✓	✓	✓	✓	✓	✓	✓
Redundant and energy-efficient cooling using direct free cooling and climate controls	✓	✓	✓	✓	✓	✓	✓	✓
Cold-aisle containment in above-average raised flooring	✓	✓	✓	✓	✓	✓	✓	✓
Monitoring of process-relevant parameters via intelligent measurement, control, regulation, and monitoring system	✓	✓	✓	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Fire protection								
Site-wide early warning fire system; direct connection to the local fire and rescue coordination center	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic fire protection measures	✓	✓	✓	✓	✓	✓	✓	✓
Regular training for emergencies and fire protection	✓	✓	✓	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Network and attack protection								
Redundant and highly available network infrastructure **99.9% network availability in accordance with GTC**	✓	✓	✓	✓	✓	✓	✓	✓
Continuous active DDoS recognition	✓	✓	✓	✓	✓	✓	✓	✓
Use of firewall and port management	Client's responsibility	Client's responsibility	Client's responsibility	✓	✓	✓	✓	✓
Individually configured firewall	NA	✓	✓	NA (see next line)	NA (see next line)	NA (see next line)	NA (see next line	✓
Hetzner-managed firewall with 24/7 monitoring	NA	NA (see last line)	NA (see last line)	✓	✓	✓	✓	NA (see last line)

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Backup and system protection								
Backup and recovery plan	Client's responsibility	Client's responsibility	✓ Backups and snapshots can be added for a fee	✓ partially depends on purchased services	✓	✓ Own backup recommended	Snapshots depending on purchased services	Client's responsibility Redundant storage within the cluster system
Disk mirroring	Client's responsibility	Client's responsibility	Client's responsibility	✓	✓	✓	✓	✓

X. Procedures for regular review, assessment and evaluation

Regularly testing, assessing, and evaluating the data protection and security standards ensures that the measures stay in compliance with regulations and improve over time.

Measure	Implementation
Data protection and information security management system (DMS, ISMS)	✓
Employment of a data protection and information security officer who is integrated into the operational processes	✓
Data-protection-friendly default settings (privacy by default and privacy by design)	✓
Incident response management	✓
Certifications according to ISO 27001, § 8a BSI-KritisV and BSI C5 Type 2 certification	✓
Annual review of TOMs by external service provider	✓
Annual review of the proper calculation and billing of connection charges by expert opinion in accordance with § 63 TKG	✓
EMAS certification (ISO 14001) of the environmental management system at German locations	✓

5 General information

In view of the sampling nature of the study, it should be noted that there may be other strengths, but also potential risks, outside the aspects examined in connection with this study.

Although the inspection was carried out with the greatest possible care, TÜV Rheinland i-sec GmbH therefore excludes liability for existing and unrecognised potential risks.

The test result in no way releases the company from pursuing its safety objectives.

In all cases, the company itself is responsible for the measures it takes to ensure its security objectives.

Any liability for possible damage resulting from incorrect use of the information provided here is excluded.