Report

- Confidential -

Review of the technical and organizational measures of the data centers

at the

HETZNER

Hetzner Online GmbH

Version 1.0

Report no. -6301702001

Cologne,11. Februar 2025

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 01/03/2023) • 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 that Hetzner Online GmbH complies 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 27001:2013 certified. The certification is valid until September 2025 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 of Hetzner Online GmbH."

The current certificate is available on the Hetzner Online GmbH website at: https://www.hetzner.com/de/unternehmen/zertifizierung/.

2.2 Scope of application

Data centre parks at the locations:

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

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:

Simon Beißer	IT Security Officer
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 Results in detail

I. Confidentiality (Art. 32 para. 1 lit. b GDPR)

- **Access control**
    - **Data centre parks in Nuremberg, Falkenstein and Helsinki**
        - Electronic access control system with logging
        - High security fence around the entire data centre park
        - Documented key allocation to employees and colocation customers for colocation racks (each customer exclusively for their own colocation rack)
        - Guidelines for escorting and labelling guests in the building
        - 24/7 staffing of the data centres
        - Video surveillance at entrances and exits, security gates and server rooms
        - Access to the premises for external persons (e.g. visitors) is restricted as follows: only when accompanied by a Hetzner Online GmbH employee
    - **Administration**
        - Electronic access control system with logging
        - Video surveillance at the entrances and exits
- **Access control**
    - for dedicated servers, colocation servers, cloud servers and storage boxes
        - Server passwords that were only changed by the client after initial commissioning and are not known to the contractor.
        - The password for the administration interface is assigned by the client - the passwords must fulfil predefined guidelines. In addition, the client can use two-factor authentication to further secure their account.
    - for managed servers, web hosting and storage share
        - Access is password-protected, access is only granted to authorised employees of the contractor; passwords used must have a minimum length and are renewed at regular intervals

- **Access control**
    - for internal management systems of the contractor
        - The contractor shall ensure that unauthorised access is prevented through regular security updates (in accordance with the current state of the art).
        - Audit-proof, binding authorisation allocation procedure for the contractor's employees
    - for dedicated servers, colocation servers, cloud servers and storage boxes
        - The client is responsible for access control.
    - for managed servers, web hosting and storage share
        - The contractor shall ensure that unauthorised access is prevented through regular security updates (in accordance with the current state of the art).
        - Audit-proof, binding authorisation allocation procedure for the contractor's employees
        - The client is solely responsible for transferred data/software with regard to security and updates.
- **Data carrier check**
    - **Data centre parks in Nuremberg, Falkenstein and Helsinki**
        - Hard drives are overwritten (deleted) several times after cancellation using a defined procedure. After checking, the hard disks are reinserted.
        - Defective hard drives that cannot be securely deleted are destroyed (shredded) directly in the data centre (Falkenstein).
- **Separation control**
    - for internal management systems of the contractor
        - Data is stored physically or logically separated from other data.
        - Data is also backed up on logically and/or physically separate systems.
    - for dedicated servers, colocation servers, cloud servers and storage boxes
        - The client is responsible for the separation check.
    - for managed servers, web hosting and storage share
        - Data is stored physically or logically separated from other data.
        - Data is also backed up on logically and/or physically separate systems.

- **Pseudonymisation (Art. 32 para. 1 lit. a GDPR)**
    - The client is responsible for pseudonymisation

II. Integrity (Art. 32 para. 1 lit. b GDPR)

- **Transfer control**
    - All employees are instructed within the meaning of Art. 32 para. 4 GDPR and are obliged to ensure that personal data is handled in compliance with data protection regulations.
    - Data protection-compliant deletion of data after order completion.
    - Options for encrypted data transmission are provided within the scope of the service description of the main order.
- **Input control**
    - for internal management systems of the contractor
        - The data is entered or recorded by the client himself.
        - Changes to the data are logged.
    - for dedicated servers, colocation servers, cloud servers and storage boxes
        - The client is responsible for input control.
    - for managed servers, web hosting and storage share
        - The data is entered or recorded by the client himself.
        - Changes to the data are logged.

III. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

- **Availability control**
    - for internal management systems of the contractor
        - Backup and recovery concept with daily backup of all relevant data.
        - Expert use of protection programmes (virus scanners, firewalls, encryption programmes, SPAM filters).
        - Use of hard disc mirroring for all relevant servers.
        - Monitoring of all relevant servers.

    - Use of uninterruptible power supply, emergency power system.
    - Permanently active DDoS protection.

- for dedicated servers, colocation servers, cloud servers and storage boxes
    - Data backup is the responsibility of the client.
    - Use of uninterruptible power supply, emergency power system.
    - Permanently active DDoS protection.

- For managed servers, web hosting and storage share
    - Backup and recovery concept with daily data backup depending on the services booked for the main order.
    - Use of hard disc mirroring.
    - Use of uninterruptible power supply, emergency power system.
    - Use of software firewall and port regulations.
    - Permanently active DDoS protection.

- **Rapid recoverability (Art. 32 para. 1 lit. c GDPR)**
    - An escalation chain is defined for all internal systems, which specifies who is to be informed in the event of a fault in order to restore the system as quickly as possible.

IV. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- The data protection management system and the information security management system were combined to form a DIMS (Data Protection Information Security Management System).
- Incident response management is in place.
- Data protection-friendly default settings are taken into account in software developments (Art. 25 (2) GDPR).

- **Order control**
    - Our employees are instructed in data protection law at regular intervals and are familiar with the procedural instructions and user guidelines for data processing on behalf of the client, also with regard to the client's right to issue instructions. The

GTC contain detailed information on the type and scope of the commissioned processing and utilisation of the client's personal data.

- The GTC contain detailed information on the purpose limitation of the client's personal data.
- Hetzner Online GmbH has appointed a company data protection officer and an information security officer. Both are integrated into the relevant operational processes through the data protection organisation and the information security management system.

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 of 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.

6