TÜVRheinland®
Genau. Richtig.

Report

- Confidential -

Inspection of the technical and organisational measures of the data centres

for

Hetzner Online GmbH

Version 1.0_EN

Report no. 63014781-01

Cologne, the 01. March 2023

TÜV Rheinland i-sec GmbH

General information about the performed examination

Client:	Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen
Delegated 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 inspectipon:	Review of the technical and organizational measures of the data centers at the locations: • Nuremberg (Last site inspection on 25.01.2019, last inspection remote in 2021). • Falkenstein (Vogtl.) (Last site visit on 27.01.2022) • Helsinki (Tuusula, Finland) (Last site visit on 01.03.2023)
Supplied documents:	Order Data Processing Agreement incl. Annex 2: Technical and Organizational Measures according to Art. 32 DS-GVO of Hetzner Online GmbH
Project Manager:	Bernd Zimmer

Project Manager

Cologne, the 01. March 2023

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 organizational measures taken in accordance with Article 28 of the GDPR. The audit was based on the generally accessible technical and organizational measures, available at https://www.hetzner.com/AV/TOM.pdf. The aforementioned technical and organizational measures are part of the order processing contract between Hetzner Online GmbH (contractor) and the customer (client).

No discrepancies were found during the audit.

2 Basics and methodology

This section describes the initial situation, scope, objectives, and test and evaluation basis of the study conducted.

2.1 Initial situation and objective

The company Hetzner Online GmbH is active on the market in the area of hosting and housing as a processor within the meaning of Art. 28 DS-GVO. Within the scope of this activity, DS-GVO-compliant order processing contracts are concluded with the customers. The contracts include technical and organizational measures (pursuant to Art. 28 (3) e of the 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 certification. The certification is valid until September 2025 and covers all locations in Germany and Finland. The scope of the certificate is stated as:

"The scope of the information security management system includes all hosting services and the data centers of Hetzner Online GmbH."

The current certificate and the declaration of applicability are available on the website of Hetzner Online GmbH at: https://www.hetzner.com/de/unternehmen/zertifizierung/.

2.2 Scope

Data center parks at the sites:

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

2.3 Test/audit basis

The test bases used were:

- Technical and organizational measures of the company Hetzner Online GmbH, which can be accessed under the link https://www.hetzner.com/AV/TOM.pdf.
- EU General Data Protection Regulation (EU GDPR)

2.4 Procedure

As part of a site visit, the technical and organizational measures at the sites were traced on the respective test date and their conformity with the specifications of 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 people were interviewed during the audit:

Margit Müller	Data Protection Coordinator
Simon Biter	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 order pursuant to Art. 28 DS-GVO: Technical and organizational measures pursuant to Art. 32 DS-GVO and Annex*" have been implemented and correspond to the contractually assured measures.

4 Results in detail

I. Confidentiality (Art. 32 para. 1 lit. b DS-GVO)

- **Physical access control**
    - **Data center parks in Nuremberg, Falkenstein and Helsinki**
        - electronic access control system with logging
        - High security fence around the entire data center park
        - documented key allocation to employees and colocation customers for colocation racks (each customer exclusively for his colocation rack)
        - Guidelines for escorting and identifying guests in the building
        - 24/7 staffing of the data centers
        - Video surveillance at entrances and exits, security gates and server rooms
        - Access to the premises for persons outside the company (e.g. visitors) is restricted as follows: only in the company of a Hetzner Online GmbH employee
    - **Monitoring**
        - electronic access control system with logging
        - Video surveillance at the entrances and exits
- **Logical access control**
    - for Dedicated Server, Colocation Server, Cloud Server and Storage Box
        - Server passwords, which have been changed only by the Client after the initial start-up and are not known to the Contractor.
        - The password to the administration interface is assigned by the client - the passwords must meet predefined guidelines. In addition, two-factor authentication is available there for the client to further secure his account.
    - for Managed Server, Webhosting and Storage Share
        - Access is password protected, access is only available to authorized employees of the contractor; passwords used must be of minimum length and are renewed at regular intervals

- **Logical access control (internal systems)**
    - for internal management systems of the contractor
        - By means of regular security updates (in accordance with the respective state of the art), the Contractor shall ensure that unauthorized access is prevented.
        - Audit-proof, binding authorization allocation procedure for contractor employees
    - for Dedicated Server, Colocation Server, Cloud Server and Storage Box
        - The client is responsible for access control.
    - for Managed Server, Webhosting and Storage Share
        - By means of regular security updates (in accordance with the respective state of the art), the Contractor shall ensure that unauthorized access is prevented.
        - Audit-proof, binding authorization allocation procedure for contractor employees
        - The client is solely responsible for transferred data/software in terms of security and updates.
- **Transfer control**
    - **Data center parks in Nuremberg and Falkenstein and Helsinki**
        - Hard disks are overwritten (erased) several times after termination using a defined procedure. After verification, the hard disks are inserted again.
        - Defective hard disks that cannot be safely erased are destroyed (shredded) directly in the data center (Falkenstein).
- **Separation control**
    - for internal management systems of the contractor
        - Data is stored physically or logically separated from other data.
        - Data backup is also performed on logically and/or physically separated systems.
    - for Dedicated Server, Colocation Server, Cloud Server and Storage Box
        - The separation control is the responsibility of the client.

- for Managed Server, Webhosting and Storage Share
  - Data is stored physically or logically separated from other data.
  - Data backup is also performed on logically and/or physically separated systems.

- **Pseudonymization (Art. 32 para. 1 lit. a DS-GVO)**
  - The client is responsible for pseudonymization

II. Integrity (Art. 32 para. 1 lit. b DS-GVO)

- **Data transfer control**
  - All employees have been instructed in accordance with Art. 32 Para. 4 DS-GVO and are obliged to ensure that personal data is handled in accordance with data protection regulations.
  - Data deletion in accordance with data protection regulations after completion of the order.
  - Possibilities 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 Server, Colocation Server, Cloud Server and Storage Box
    - The responsibility of the input control is incumbent on the client.
  - for Managed Server, Webhosting 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 DS-GVO)

- **Availability control**
    - for internal management systems of the contractor
        - Backup and recovery concept with daily backup of all relevant data.
        - Expert use of protection programs (virus scanners, firewalls, encryption programs, SPAM filters).
        - Use disk mirroring on all relevant servers.
        - Monitoring of all relevant servers.
        - Use of uninterruptible power supply, backup power supply.
        - Permanently active DDoS protection.
    - for Dedicated Server, Colocation Server, Cloud Server and Storage Box
        - Data backup is the responsibility of the client.
        - Use of uninterruptible power supply, backup power supply.
        - Permanently active DDoS protection.
    - For Managed Server, Web Hosting and Storage Share
        - Backup and recovery concept with daily backup of data depending on the booked services of the main order.
        - Use of hard disk mirroring.
        - Use of uninterruptible power supply, backup power supply.
        - Use of software firewall and port regulations.
        - Permanently active DDoS protection.
- **Rapid recoverability (Art. 32(1)(c) DS-GVO)**
    - An escalation chain is defined for all internal systems, specifying who is to be informed in the event of an error in order to restore the system as quickly as possible.

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

- The data protection management system and the information security management system were combined into 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 they 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 about the type and scope of the commissioned processing and use of the client's personal data.
  - The GTC contain detailed information about 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 organization and the information security management system.

5 General notes

With regard to the sample nature of the investigation, it should be noted that there may be other strengths, as well as potential risks, outside of the aspects reviewed in the context of this investigation.

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

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

In any case, the company is responsible for its own measures to ensure its safety objectives.

Any liability for possible damages resulting from incorrect use of the information given here is excluded.