TÜVRheinland®
Genau. Richtig.

Report

- Confidential -

Inspection of the technical and organisational measures of the data centres

for

Hetzner Online GmbH

version 1.0

Report No 63011273-4

Cologne, 20. Februar 2020

TÜV Rheinland i-sec GmbH

General information on the study carried out

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: i-sec@i-sec.tuv.com
Scope of inspectipon:	Review of the technical and organisational measures of the computer centres at the locations: • Nuremberg (last site visit on 25.01.2019) • Falkenstein (Vogtl.) (last site visit on 28.01.2020) • Helsinki (last site visit on 20.02.2020)
Other applicable documents:	Data processing agreement including Annex 2: Technical and organisational measures according to Art. 32 GDPR of Hetzner Online GmbH
Project manager:	Bernd Zimmer
Project team members:	-

Project Manager

Cologne, 20. Februar 2020

No part of this document may be reproduced.

Table of contents

1 Summary

The TÜV Rheinland i-sec GmbH confirms to Hetzner Online GmbH that the information provided to the client regarding the technical and organizational measures taken in accordance with Art. 28 GDPR. This was verified by site inspections at the locations Nuremberg, Falkenstein (Vogtl.) and Helsinki (Finland) as well as interviews on site. The site inspections were carried out on 28.01.2020 (Falkenstein) and 20.02.2020 (Helsinki) and were based on the generally accessible technical and organisational measures, available at https://www.hetzner.com/AV/TOM_en.pdf. The aforementioned technical and organizational measures are part of the order processing contract between Hetzner Online GmbH (contractor) and the client (client). The last inspection of the data center park in Nuremberg took place on 25.01.2019.

No deviations were found during the audit.

2 Basics and methodology

This section describes the initial situation, scope, objectives and the basis for testing and evaluation of the study carried out.

2.1 Initial situation and objectives

The company Hetzner Online GmbH is active on the market in the area of hosting or housing as a contract processor in the sense of Art. 28 GDPR. Within the scope of this activity, GDPR-compliant contract processing agreements are concluded with customers. The contracts include (in accordance with Art. 28 Para. 3 lit. e GDPR) technical and organisational measures which are the subject of this review.

Since October 2016 Hetzner Online GmbH is certified according to the international standard ISO/IEC 27001:2013. The scope of the certificate is specified:

The scope of the information security management system covers the infrastructure, operation and customer support of the data centers.

The data centers in Helsinki are also ISO/IEC27001:2013 certified.

2.2 Scope

Data centers at the locations:

- Falkenstein/Vogtland
- Nuremberg
- Helsinki (Finland)

2.3 Test/Audit Basis

The following were used as test bases:

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

2.4 Procedure

As part of a site inspection, the technical and organizational measures at the locations were inspected on the respective inspection date and the conformity with the specifications of Hetzner Online GmbH was checked.

In addition to the site visit, 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:

Margit Müller	Data Protection Officer
Simon Beißer	IT Security Officer
Sebastian Lippold	Information Security Officer
Joonas Terhivoo	Data Center Manager (Helsinki)

3 Result of the check:

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

4 Results in detail

I. Confidentiality (Article 32(1)(b) of the GDPR)

- **Access control (physical access)**
    - **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
        - Clients for colocation racks (each client exclusively for his colocation rack)
        - Guidelines for the escort and identification of guests in the building
        - 24/7 staffing of the computer centres
        - Video surveillance at the entrances and exits, security gates and server rooms Access to the rooms 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 inputs and outputs
- **Access control (logical access)**
    - for Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Server passwords, which have only been changed by the client after the initial start-up by himself and are not known to the contractor.
        - The password to the administration interface is assigned by the client himself - the passwords must meet predefined guidelines. In addition, a two-factor authentication is available to the client there 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 have a minimum length and are renewed at regular intervals

- **Access control**
    - for internal management systems of the contractor
        - By means of regular security updates (according to the current state of the art), the contractor ensures that unauthorized access is prevented.
        - Audit-proof, binding authorisation procedure for employees of the contractor
    - for Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - The responsibility for access control lies with the client.
    - for Managed Server, Webhosting and Storage Share
        - By means of regular security updates (according to the current state of the art), the contractor ensures that unauthorized access is prevented.
        - Audit-proof, binding authorisation procedure for employees of the contractor
        - For transferred data/software, only the customer is responsible for security and updates.

- **Data media control**
    - **Data centre parks in Nuremberg and Falkenstein and Helsinki**
        - Hard disks are overwritten (deleted) several times after termination using a defined procedure. After checking, the hard disks are inserted again.
        - Defective hard disks that cannot be securely deleted are destroyed (shredded) directly in the data center (Falkenstein).

- **Separation control**
    - for internal management systems of the contractor
        - Data is stored physically or logically separate from other data.
        - Data backup is also performed on logically and/or physically separate systems.
    - for Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Separation control is the responsibility of the client.
    - for Managed Server, Webhosting and Storage Share
        - Data is stored physically or logically separate from other data.
        - Data backup is also performed on logically and/or physically separate systems.

- **Pseudonymisation (Article 32(1)(a) GDPR)**
    - The client is responsible for the pseudonymisation

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

- **Transfer control**
    - All employees are instructed in accordance with Article 32 Paragraph 4 GDPR and are obliged to ensure that personal data is handled in compliance with data protection regulations.
    - Deletion of the data in accordance with data protection regulations after completion of the order.
    - Possibilities for encrypted data transmission are made available 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.
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - The responsibility for input control lies with 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 (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 programs (virus scanners, firewalls, encryption programs, SPAM filters).

- Use of hard disk mirroring for all relevant servers.
- Monitoring of all relevant servers.
- Use of uninterruptible power supply, emergency power system.
- Permanently active DDoS protection.

- für Dedicated Server, Colocation Server, Cloud Server und Storage Box“
  - Data backup is the responsibility of the client.
  - Use of uninterruptible power supply, emergency power system.
  - 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 contract.
  - Use of hard disk mirroring.
  - Use of uninterruptible power supply, emergency power system.
  - Use of software firewall and port regulations.
  - Permanently active DDoS protection.

- **Rapid recoverability (Art. 32 (1) lit. c GDPR);**
  - An escalation chain is defined for all internal systems, which specifies 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) lit. d GDPR; Art. 25 (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 available.
- Data protection-friendly default settings are taken into account in software developments (Art. 25 (2) GDPR).

- **Order control**

    - Our employees are instructed at regular intervals in data protection law 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 give instructions. The general terms and conditions contain detailed information on the type and scope of the commissioned processing and use of personal data of the client.

    - The GTC contain detailed information about the purpose limitation of the personal data of the client.

    - 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 sampling nature of the investigation, it should be noted that there may be other strengths but also potential risks outside the aspects examined in the context of this investigation.

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

The test result does not in any way release the company from pursuing its security objectives.

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

Any liability for possible damages resulting from a wrong application of the information given here is excluded.

No part of this document may be reproduced.