- Confidential -

Report

Audit of the technical and organisational measures

at

Hetzner Online GmbH
Industriestraße 25
91710 Gunzenhausen

Version 1.0

Report Nr. 63010063-1

Cologne, 25.01.2019

TÜV Rheinland i-sec GmbH

TÜVRheinland®
Genau. Richtig.

General information about the audit

Client:	Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen
Contractor:	TÜV Rheinland i-sec GmbH Unternehmensgruppe TÜV Rheinland Group Competence Center IT Prozesse / IT Security 51105 Köln Tel. 0221 - 806 4059 / Fax 0221 - 806 1580 E-Mail: i-sec@de.tuv.com
Scope:	Technical and organisational measures at the locations in Nuremberg and Falkenstein (Vogtl.) based on GDPR.
Applicable Documents:	Hetzner Online GmbH data processing agreement
Project Leader:	Bernd Zimmer
Project Employee:	-

Project Leader

Cologne, 25. January 2019

Index

1 Summary

TÜV Rheinland i-sec GmbH confirms, that Hetzner Online GmbH has implemented the technical and organisational measures that are documented and provided to the customers as part of the data processing agreement according to Art. 28 Sec. 2 GDPR.
The audit was conducted at the location in Nuremberg by an on-site inspection as well as an interview
The on-site inspection was conducted on 25.01.2019 and was based on the publicly available document „Technical and Organisational Measures in accordance with Art. 32 GDPR from https://www.hetzner.com/AV/TOM_en.pdf.

2 Principles and methodology

2.1 Initial situation and objective

Hetzner Online GmbH provides Hosting and Housing to their customers as a service according to Art. 28 GDPR. Data processing agreements between Hetzner and the customers are in place. The agreement contains the required information (Art. 28 Sec. 3 lit. e GDPR) incl. technical and organisational measures (Art. 32 GDPR), that are the basis of the audit.

Hetzner Online GmbH holds an ISO/IEC 27001:2013 certificate, since October 2016. The scope of the certificate is:

Data center infrastructure –operation, Server setup in the locations Nuremberg and Falkenstein.

2.2 Scope

Data centers in:

- Falkenstein/Vogtland
- Nuremberg

2.3 Basis for the audit

As basis for the audit was used:

- Technical and organisational measures of Firma Hetzner Online GmbH, available under https://www.hetzner.com/AV/TOM_en.pdf
- EU GDPR

2.4 Approach

The technical and organisational measures were audited in an onsite-inspection at the data center in Nuremberg. The measures were checked against the specifications made by Hetzner online GmbH.

List of participants:

Margit Müller Data Protection Officer

Simon Beißer IT Security Officer

Sebastian Lippold Information Security Officer

3 Audit Result

The documented technical and organizational measures “Appendix 2 of the Agreement Pursuant to Art. 28 GDPR: Technical and Organizational Measures in Accordance with Art. 32 GDPR and Amendments“ are implemented and correspond to the contractually guaranteed measures.

4 Results in detail

I. Confidentiality

- **Physical access control**
  - **Data center parks in Nürnberg and Falkenstein**
    - electronic physical entry control system with log
    - high security perimeter fencing around the entire data center park
    - documented distribution of keys to employees and colocation customers for colocation racks (each Client only for his rack)
    - policies for accompanying and designating guests in the building
    - data center staff present 24/7
    - video monitoring at entrances and exits; security door interlocking systems and server rooms
    - For people outside of the employment of Hetzner Online GmbH (data center visitors), entrance to the building is only permitted in the company of a Hetzner Online employee.
  - **Monitoring**
    - electronic physical access control system with log
    - video surveillance for all entrances and exits

- **Electronic access control**
  - for dedicated root server, colocation server, and cloud server principal commissions
    - server passwords, which, after the initial deployment, can only be changed by Client and are not known to the Supplier
    - The Client’s password for the administration interface is determined by the Client himself; the password must comply with predefined guidelines. In addition, the Client may employ two-factor authentication to further secure his account.
  - for managed server, web hosting, and storage box principal commissions
    - Access is password-protected and only employees of the Supplier have access to the passwords. Passwords must meet a minimum length, and new passwords shall be changed on a regular basis.

- **Internal access control**
  - for the Supplier's internal administration systems
    - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
    - a revision-proof, compulsory process for allocating authorization for Supplier employees
  - for dedicated root server, colocation server, and cloud server principal commissions

        - The responsibility for access control is incumbent upon the Client.
    - for managed server, web hosting, and storage box principal commissions
        - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
        - a revision-proof, compulsory process for allocating authorization for Supplier employees
        - Only the Clieent is responsible for transferred data/software with regard to security and updates.

- **Transfer control**

    - **Data center parks in Nürnberg and Falkenstein**
        - Drives that were in operation on canceled servers will be swiped multiple times (deleted) in accordance with data protection polices upon termination of the contract. After thorough testing, the swiped drives will be reused.
        - Defective drives that cannot be securely deleted shall be destroyed (shredded) directly in the Falkenstein data center.

- **Isolation control**

    - for the Supplier's internal administration systems
        - Data shall be physically or logically isolated and saved separately from other data.
        - Backups of data shall also be performed using a similar system of physical or logical isolation.
    - for dedicated root server, colocation server, and cloud server principal commissions
        - The Client is responsible for isolation control.
    - for managed server, web hosting, and storage box principal commissions
        - Data shall be physically or logically isolated and saved separately from other data.
        - Backups of data shall also be performed using a similar system of physical or logical isolation.

- **Pseudonymization**

    - The Client is responsible for pseudonymization.

II. Integrity (Art. 32 Para.1 Clause b GDPR)

- **Data transfer control**

    - All employees are trained in accordance with Art. 32 Para. 4 GDPR and are obliged to ensure that personal data is handled in accordance with data

protection regulations.
- Deletion of data in accordance with data protection regulations after termination of the contract.
- Encrypted data transmission options are provided within the scope of the service description of the principal commission.

- **Data entry control**

  - for the Supplier's internal administration systems
    - Data is entered or collected by the Client.
    - Changes in data are logged.
  - for dedicated root server, colocation server, and cloud server principal commissions
    - The responsibility for input control is incumbent upon the Client.
  - for managed server, web hosting, and storage box principal commissions
    - Data is entered or collected by the Client.
    - Changes in data are logged.

III. Availability and Resilience (Art. 32 Para. 1 Clause b GDPR)

- **Availability control**

  - for the Supplier's internal administration systems
    - backup and recovery concept with daily backups of all relevant data
    - professional employment of security programs (virus scanners, firewalls, encryption programs, spam filters)
    - employment of disk mirroring on all relevant servers
    - monitoring of all relevant servers
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for dedicated root server, colocation server, and cloud server principal commissions
    - Data backup is incumbent upon the Client.
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for managed server, web hosting, and storage box principal commissions
    - backup and recovery concept with daily backups of all relevant data depending upgon the services booked for the principal commission
    - employment of disk mirroring
    - employment of an uninterruptible power supply system or emergency power supply system
    - employment of software firewalls and restricted ports
    - permanently active DDoS protection

- **Rapid recovery measures (Art. 32 Para. 1 Clause c GDPR)**

    - For all internal systems, there is a defined escalation chain 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 testing, assessment, and evaluation (Art. 32 Para. 1 Clause d GDPR; Art. 25 Para. 1 GDPR)

- The data protection management system and the information security management system have been combined into a DIMS (data protection information security management system).
- Incident response management is available.
- Data-protection-friendly default settings are taken into account for software development (Art. 25 Para. 2 GDPR).

- **Agreement or contract control**

    - Hetzner Onling GmbH employees are regularly instructed in data protection law 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 of instruction. The General Terms and Conditions contain detailed information on the type and scope of the commissioned data processing and use of the Client's personal data.
    - The General Terms and Conditions contain detailed information about the purpose limitation of Client’s personal data.
    - Hetzner Online GmbH has appointed a company Data Protection Officer and an Information Security Officer. The data protection organization and the information security management systems integrate both officers into the relevant operational procedures.

5 General Information

With regard to the sample characteristics of the survey it is advised, that outside of the assessed aspects in relation with this survey, there may be other strengths, but also other potential risks too.

Although the assessment is liable to maximum accuracy, the TÜV Rheinland i-Sec GmbH excludes liability for present and not detected potential risks.

The assessment result does absolve the company in no way from the follow up of their security objectives.

In every case the company is self-responsible for their actions to ensure their security objectives.

Every liability for possible damages, which result from the incorrect execution of the here given information, is excluded.