Technical and organisational measures (TOMs)

SEMKNOX will perform the data processing at two locations: on the premises of the Hetzner GmbH service provider (server hoster) and in its own offices. For this reason, reference will be made to the TOMs of Hetzner GmbH in several aspects.

§ 1.Confidentiality

a. Physical access control

For the TOMs relating to physical access control on the Hetzner service provider's premises, refer to that company's TOMs.

For the offices at SEMKNOX, physical access control is ensured by locks at the main office entrance. Visitors are only admitted when accompanied by employees. Only permanent staff have keys to the offices.

b. Network logon control

For the TOMs relating to network logon control on the Hetzner premises, refer to that company's TOMs.

After the server processing by SEMKNOX, access to the servers is only allowed through SSH access with user name and password. Access is only granted to permanent SEMKNOX staff. Each server has a different password. Server accesses are recorded in the system logs. The use of byobu enables the traceability of the activities of employees.

All persistent server storage is fully encrypted with AES512. Access to the servers is encrypted whenever possible.

Open ports are only made accessible to specific IP addresses via a firewall (iptables).

Personal data is stored in databases protected by additional user names and passwords.

c. Access control

File accesses become visible in byobu. The system logs also protocol violations of existing authorisation settings.

If any employees with access to the servers leave the company, the password is changed.

When encrypted data media are disposed of, they are formatted and rendered unreadable by overwriting the key.

d. Separation

For the TOMs relating to the separation control on the Hetzner service provider's premises, refer to that company's TOMs.

SEMKNOX separates customer data using a unique identification (the so-called customer ID). All data records are provided with such customer IDs and are always only used in the context of processing the respective customer.

API accesses require both the customer ID and the apiKey to obtain access to the corresponding data.

Altogether, SEMKNOX operates a minimum of two service environments per product – namely a development and a productive environment. This way, it is possible to ensure that new developments are sufficiently tested.

e. Pseudonymisation & Encryption

All persistent storage is encrypted with AES512.

§ 2.Integrity

a. Entry control

All employers are instructed within the meaning of Article 32 Section 4 DS-GVO General Data Protection Regulation) and are bound to conform to the data protection provisions when handling personal data.

API accesses are logged. This makes it possible to see who has entered

which personal data in the system when.

All SEMKNOX employees have access to this log data, which is deleted at irregular intervals.

b. Transfer control

Data is transmitted to the API via HTTPS and downloaded from the API via HTTPS. In these processes, the data is protected by the respective SSL connection.

§ 3.Availability and resilience

a. Availability control

For the TOMs relating to the availability control on the Hetzner service provider's premises, refer to that company's TOMs.

In addition, SEMKNOX operates load balancers, which enable switching between several servers to ensure the availability of services at all times.

A continual synchronisation set up between the live and backup systems provides for a current data status.

§ 4.Procedures for regular checking, evaluation and assessment

For the TOMs relating to the procedures for regular checking, evaluation and assessment on the Hetzner service provider's premises, refer to that company's TOMs.

Furthermore, SEMKNOX provides instruction to its employees on the subject of data protection. On joining the company, all employees are instructed in the procedures for handling personal data. In addition, each employee is also bound in writing to confidentiality after ending his employment with us.

If an employee detects a data protection violation, then this shall be promptly reported to enable management to initiate countermeasures.

Furthermore, SEMKNOX maintains a comprehensive data protection

documentation and has established the required data protection procedures, which undergo regular checking and updating.