Technical and organizational measures (TOMs)

These technical and organization measures describe the implementation of measures for secure processing of personal data in accordance with applicable data protection legislation. The requirements of articles 24, 25 and 32 of the GDPR are taken into account as far as applicable. Below specifications apply for the following physical locations: Corporate headquarters Checkmk GmbH in Munich (GER) and Checkmk Inc. in Atlanta (U.S.), data center location, employee home offices (exception: physical access).

1. Confidentiality

1.1. Physical access

1.1.1. General concept:
All rooms in which personal data is processed or processing equipment is stored must be done in accordance with the latest version of the physical security policy. Main data processing assets are housed in an external data center holding certifications according to relevant industry standards as indicated in

Detailed measures implementing the concept at the company: The main assets for storing and processing data reside in an external data center (“DC”), certified or attested at least according to ISO 9001, ISO 27001 ,ISO 22301, ISO 27701, ISO 27017, ISO 27018, SOC 2 Type II. Applications offered as “Software as a Service” are hosted in the data centers of Amazon Web Services; see also:
https://aws.amazon.com/compliance/data-center/controls/. For any conflicts between the measures indicated below and measures listed in the Amazon Web Services website, the latter shall take precedence).

- Locked building (except Atlanta office)
- Locked office
- Electronic security locking system
- Mechanical security locking system
- Physical access control system
- Role-based physical access controls
- Biometric access control system (DC only)
- Locked server rooms
- Locked server cabinets
- Locked server rooms with access control (DC only)
- Video surveillance (DC only)
- Alarm system (DC only)
- Documented key distribution
- Central reception area
- Visitor registration
- Supervision of visitors
- Visitor identification via badge
- Definition of security perimeters
- 24/7 security staff onsite (DC only)
- Physical security policy

1.2. Authentication

1.2.1. General concept: Unique user accounts are created for each individual user and must be protected with a password of sufficient length and complexity. Password rules are centrally enforced and login attempts tightly monitored. Key applications require a secure connection and 2-factor authentication. Access to administrative interfaces is limited to a minimal group of IT administrators and requires multi-factor authentication and an encrypted connection. The use of company assets is regulated by an acceptable use policy.

1.2.2. Key measures implementing the concept at the company. Please review the latest version of the appropriate policies as indicated below for additional details:

- Unique user accounts
- Centrally managed authentication with username and password
- Password convention requiring complex passwords with at least 12 characters
- Automated control of password convention
- Multi-factor-authentication for key applications
- Multi-factor authentication for administrative interfaces
- Blocking of access after repeated incorrect entry of login data
- Disk encryption on endpoints
- Requirement of VPN connection for access to data processing applications
- Implementation of an endpoint management software or comparable control
- Implementation of a mobile device management software
- Implementation of an up-to-date firewall in endpoints
- Implementation of an up-to-date anti-virus or compensating controls
- Centralized log management
- Verification of user identities
- Periodic account reviews
- Access control policy
- Acceptable use policy
- Password policy
- Cryptography policy

1.3. Data access control

1.3.1. General concept:
A role-based authorization concept is in place. Access to personal data is restricted to authorized personnel and limited to the extent needed for them to fulfill their task (principle of least privilege). Administrative access is limited to a minimal group of IT administrators. The access to user access logs of our Software as a Service applications is limited to auditors and security engineers. The assignment, modification and withdrawal of access privileges follow a documented process. Privileges are subject to regular review. To protect data from unauthorized access, all personal data at rest and in transit is encrypted. Retention of personal data as well as their

deletion or destruction follows documented procedures and recognized industry standards. Removable storage media will generally not be used for personal data.

1.3.2. Detailed measures implementing the concept at the company:

- Central management of application access per user or group, where possible
- Authentication via username and password
- Logging of user access to sensitive services or applications
- Encryption of data at rest and in transit
- Deletion of storage media in accordance with the Information retention policy
- Destruction of physical documents in accordance with the Information retention policy
- Locked cabinets to store physical documents
- Privacy screens and view guards for sensitive functions
- Role-based authorization concept for applications and files in accordance with least privilege principle
- Regular review and adaptation of access rights
- Limitation and documentation of administrative access
- Documented procedures for the retention and deletion of personal data
- Information classification policy
- Information retention policy
- Acceptable use policy
- Clean desk and clear screen requirement
- General prohibition to store company data on removable storage media in accordance with the

Acceptable use policy Specific measures for applications offered as "Software as a Service":

- Access to user access logs limited to Auditors and Security Engineers

1.4. Pseudonymization

1.4.1. General concept:
Personal data is pseudonymized wherever this is possible at early stages of analyses. Third parties are advised to pseudonymize or anonymize data at source if personal information is not required for processing.

1.4.2. Detailed measures implementing the concept at the company:

- Utilization of hashing algorithms where applicable and necessary
- Advice to third parties to pseudonymize data at source
- Pseudonymization at an early stage of data processing where necessary
- Immediate pseudonymization upon request

1.5. Separation control

1.5.1. General concept:

Personal data is separated by the Customer using at least logical separation. In our Software as a Service applications, we implement a multi-tenancy concept with logical separation of data storage.

1.5.2. Detailed measures implementing the concept at the company:

- Logical separation of live and test environments
- Physical or logical separation of applications
- Logical separation of internal networks by business functions
- Logical separation of client data in applications
- Logical separation of tenants (SaaS only)
- Role-based access controls
- Limitation of direct access to databases

Specific measures for applications offered as “Software as a Service”:

- Logical separation of tenants
- Logical separation of storage of tenant data

2. Integrity

2.1. Transfer control

2.1.1. General concept:
Measures are in place to assign the entry, modification and deletion of personal data to the individual performing them. The modification and deletion of data records must be restricted so that accidental modification or deletion is effectively prevented.

2.1.2. Detailed measures implementing the concept at the company:
TLS encryption of all data in transit

- VPN connection for access to core applications
- Prohibition to use private storage media for company data
- Prohibition to use company communication accounts for private purposes
- Prohibition to store company data on unmanaged private assets
- Encryption of data on storage media
- General prohibition to store company data on removable storage media
- Anonymization and pseudonymization, where applicable

2.2. Input control

2.2.1. General concept:
Measures are in place to assign the entry, modification and deletion of personal data to the individual performing them. The modification and deletion of data records must be restricted so that accidental modification or deletion is effectively prevented.

2.2.2. Detailed measures implementing the concept at the company:

- Trace ability of entries, changes and deletions through personalized users
- Documented procedures for assigning, changing and withdrawing user authorizations

- Logging of modifications to personal data
- Role-based access controls
- Separation of duties

2.3. Order control

2.3.1. General concept:
As part of the order control, all data processing operations carried out on behalf of the Customer are carried out exclusively upon written instructions of the Customer. All employees involved in data processing activities are regularly trained. Sub-processors are only engaged as agreed with the customer. They are diligently selected according to a documented supplier evaluation and management process. All sub-processors are required to sign a Data Processing Agreement in accordance with article 28 of the GDPR.

2.3.2. Detailed measures implementing the concept at the company:

- Documentation of processing activities
- Processing of personal data only upon written consent
- Ensuring that data is destroyed or returned in compliance with data protection regulations after completion of the processing assignment
- Diligent evaluation and selection of data processors
- Obligation of all data processors in accordance with article 28 of the GDPR
- Written agreement with the processor on the minimum data protection standard
- Explicit regulation on the engagement of further sub-processors
- Authorization to perform audits at processors, where possible
- Risk-based monitoring of processors
- Supplier management policy

3. Availability and resilience

3.1. General concept:
Measures to effectively prevent downtimes due to physical disruption are implemented in all data centers (e.g., uninterruptible power supply, smoke and fire detection, air conditioning). Documented business continuity and emergency plans are in place.

3.2. Detailed measures implementing the concept at the company:
The main assets for storing and processing data reside in an external data center see also 1.1.2.

- Regular, automated and documented patch management for servers
- Regular, centrally administered and documented patch management for endpoints, adapted to the operating system
- Automated vulnerability scanning and alerting
- Use and regular updating of an anti-virus software or compensating controls
- Data storage on storage system

- Capacity monitoring and alerting
- Spatially redundant data storage (data center only)
- Redundant network carrier (data center only)
- Uninterruptible power supply / UPS (data center only)
- Emergency power supply (data center only)
- Redundant air conditioning of servers (data center only)
- Temperature and humidity monitoring in server rooms (data center only)
- Early smoke and fire detection (data center only)
- Fire extinguishers available in all server rooms (data center only)
- Emergency plan and business continuity policy
- Documented incident response procedures and management

4. Procedures for regular review, assessment and evaluation

4.1. General concept:
Skilled personnel has been appointed as data protection and information security officers and entrusted with the maintenance, review and regular update of the internal processes and procedures. Documented processes are in place for risk assessment and treatment as well as incident management and reporting.
All employees are contractually obliged to data secrecy and must participate in regular awareness training sessions.

4.2. Detailed measures implementing the concept at the company:

- Appointment of a data protection officer
- Appointment of an information security officer
- Contractual obligation to data protection for personnel in charge of data processing
- Regular documented awareness training of employees
- Documented procedure for the introduction, modification and decommissioning of data processing activities
- Regular review of the state-of-the-art in accordance with article 32 of the GDPR
- Documented risk assessment and treatment process with regular risk assessments