Technical and organizational measures (TOM) at seca

Presentation of technical and organizational measures at seca in accordance with Art. 32 DSGVO.

Note: seca is currently establishing an information security management system in accordance with ISO / IEC 27001 with the aim of certification. The structure of the technical and organizational measures mentioned in this appendix is based on Appendix A of ISO / IEC 27001, which lists very extensive technical and organizational measures.

A. Pseudonymization and encryption (Art. 32 (1) (a) GDPR)

Cryptography

- Use of e-mail encryption (TLS 1.2) and secure messaging methods
- Secure key management
- Pseudonymization in the processing of study data
- Pseudonymization in log files

B. Confidentiality, integrity, availability and resilience of systems and services (Art. 32 (1) (b) GDPR)

Information security organization

- Use of central software for smartphone administration
- Possibility of remote deletion of data on the mobile devices
- Use of central software for smartphone administration
- Possibility of remote deletion of data on the mobile devices

Personnel safety

- Employee commitment to data privacy and information security policies
- Clean Desk Policy and Clear Screen Policy
- Regular training on data protection and information security, including phishing and how to deal with unused devices and how to deregister service that is no longer in use and how to handle authentication information, keys and transponders

Value management

- IT equipment registration
- Documentation of the issue and return of IT equipment
- Document control policy with the definition of confidentiality levels and appropriate marking of documents
- Commissioning of shredders with data protection seal for the destruction of files and electronic data carriers

Access control

- Implementation of a policy for access allocation according to a rights-role model
- Matrix for assigning user profiles to IT systems
- Allocation of rights according to the "need to know" principle
- Formalized process for granting rights with obtaining approval from the respective supervisor
- Deletion of the user or revocation of user rights when leaving the company
- Adjustment of user rights in case of change of responsibility
- Single sign-on system for all essential applications

- Read/write permission concepts for drives and files as well as individual pages and areas in the internal wiki
- Read/write permission concepts for ticket systems
- Central management of rights via the Microsoft Active Directory service
- Change passwords every 72 days
- Password policy including password length, complexity, history, validity
- Need to change an initial password at the first login
- Allocation of additional user accounts for administrators (in addition to their personal user account)
- basically no domain or local administrator rights for users (exception: local administrator rights for computers in a specially partitioned developer network)
- transponder-secured access to printers and individual printer queues
- Logging of incorrect login attempts
- Blocking of the user account if the maximum number of failed attempts is exceeded
- Two-factor authentication for IT administrators
- Restricting the use of applications through PC management
- Access to source code of programs in the Research & Development department only for the developers

Physical and environmental safety

- Alarm system for particularly sensitive areas (including server rooms)
- Video surveillance of access to particularly sensitive areas
- Protection by motion detectors and light barriers
- Reception desk manned during business hours in the entrance area
- Recording of visits by external persons (visitor list and badges)
- Accompaniment of visitors by employees on the plant premises
- Employee-specific access authorization via transponder locking system
- Placement of server rooms in specially selected locations to protect against unauthorized access, water or fire damage, lightning strikes, etc.
- Placement of redundant server rooms in different buildings
- Knowledge of the existence and activity in particularly sensitive areas (including server rooms) according to the "need to know" principle
- Particularly sensitive areas are not recognizable as such and are not directly accessible from the outside
- External access to server rooms only with escort
- Air conditioning and monitoring of temperature and humidity in server rooms
- Fire extinguisher and fire alarm system
- physically protected laying of the cables
- Locked distribution cabinets or rooms in special areas.
- Scrapping of data media generally via specialized service provider

Communication security

- Designation of persons responsible for the network and involvement of a selected service provider for network administration
- strict rules for granting rights to access networks and network services
- consistent use of firewalls with VPN technology
- Continuous logging and monitoring of network activities
- Limitation of systems integrated in the network
- Separate developer network
- WLAN network for various purposes (e.g. separate guest WLAN)

Acquisition, development and maintenance of systems

- Development of software for self-used applications according to the same standards and processes as for medical software
- Established change control process also for self-used applications
- Processes for verification and validation of externally and self-developed applications
- Specially protected network for the development of products and self-used applications
- Specially protected test environment
- Generation of special test data instead of real data sets with personal data

Service provider and supplier relationships

- Careful selection of security and cleaning personnel
- Conclusion of order processing contracts in accordance with Art. 28 DSGVO in the case of data processing on behalf or mere data protection clauses and non-disclosure agreements in the case of other commissioning of service providers and suppliers

C. Rapid restoration of availability and access (Art. 32 (1) (c) GDPR)

Operational safety

- Resource monitoring
- Regular deletion of obsolete data to optimize storage space
- Decommissioning of applications, systems, databases or environments when the application purpose ceases to exist
- Optimization of batch processes and schedules
- Bandwidth limitation resource-intensive services (e.g., video streaming).
- Separation of development, test and operating environments for cloud services, internal applications and systems
- Web filter and download blocking
- Consistent use of antivirus software
- Subscription to relevant warning and information services
- Process for data backup according to the generation principle and regular testing of backups for recoverability
- Keeping part of the backups in an external location
- Audit log for the relevant systems used throughout the company
- Change management and approval procedures for updating applications
- Testing of the applications before installation on a test system
- Use of rollback strategies when updating applications

Information security aspects of business continuity management

- Business Continuity Management Policy
- Emergency Internet access via a second provider
- Uninterruptible power supply (UPS)

D. Regular review, assessment and evaluation of effectiveness (Art. 32 (1) (d) GDPR)

- Implementation of an information security policy and its annual review as part of quality management in accordance with ISO 9001 (already implemented) and ISO 27001 (targeted),
- Appointment of an information security officer who reports directly to management independently of IT and the other specialist departments

Handling of data protection and information security incidents

- Establishment of a data protection and information security team with a dedicated e-mail address
- Regular assessment of incidents and status quo by this team
- Advice by the external data protection officer on the assessment of a personal data breach pursuant to Art. 33, 34 GDPR with regard to measures, notification obligations and the notification of data subjects

Compliance

- Supervision of data protection and information security by the in-house legal department
- Additional assignment of a certified external data protection officer (GDDcert., CIPP/ E, CIPM)

Order control (involvement of third parties / outsourcing)

- No commissioned data processing without a corresponding contract
- Regulations on the use of further subcontractors
- Conclusion of the necessary agreements on commissioned processing in accordance with Art. 28 of the GDPR or EU standard contractual clauses for third countries (Art. 44 ff of the GDPR).

Measures in connection with cloud services

- Since seca operates SaaS services exclusively on the infrastructure of the subcontracted processor Amazon Web Services EMEA SARL (AWS), which specializes in external server hosting, at the Frankfurt am Main location, and no personal customer, employee or health data is stored or processed on seca's own premises, the above TOM in the case of SaaS shall be limited to the security measures set by Contractor on its premises.
- AWS's TOM is available at https://aws.amazon.com/de/compliance/data-center/controls/.
- seca encrypts all personal data in the SaaS services so that unauthorized access to this data is excluded.
- Seca checks the requirements of Art. 44 et seq. DSGVO in connection with the use of AWS as a service provider on a regular basis. If necessary, the appropriate guarantees required under Art. 46 DSGVO are provided, in particular in the form of standard data protection clauses.