adventics GmbH

Büro Haar bei München
Münchener Str. 23a
85540 Haar bei München

Tel. +49 (89) 4444 33 111

Email info@adventics.de
Web www.adventics.de

Status September 2023

Technical and organizational security measures of adventics GmbH

Company/ Locations

The following technical and organizational security measures relate to:

- adventics GmbH

  Münchener Str. 23A

  85540 Haar near munich, Germany
- adventics GmbH

  Seidlgasse 34

  1030 Vienna, Austria

A. Art. 32 GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, adventics GmbH shall implement appropriate technical and organizational measures to ensure a level of protection appropriate to the risk.

B. Measures to ensure confidentiality and integrity

B.1. Access control

Definition

Measures suitable to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

B.1.1. Office premises

- The office premises of adventics GmbH in Germany are located at Münchner Str.23A, 85540 Haar near Munich.
- The offices of adventics GmbH in Austria are located at Seidlgasse 34, 1030 Vienna.
- The offices are equipped with a mechanical locking system.
- The issuance of keys to employees is recorded.
- The keys are issued by the management.

B.1.2. Visitor regulations

- According to access regulations, visitors are only allowed to move around the office premises if they are accompanied by the responsible contact person at all times.

B.1.3. Access to the server room

- The adventics server rooms on which personal data is processed are located in Europe. The servers are hosted by:
  - Microsoft Azure EU Data Center Europe West/ Netherlands.

    The Azure Data Center Europe West has the following certifications: CIS Benchmark | CSA-STAR attestation | CSA-STAR certification | CSA-STAR self-assessment ISO 20000-1:2011 | ISO 22301 | ISO 27001 | ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001 PCI DSS | SOC | WCAG | CDSA | PCI DSS | Shared Assessments | TruSight | BIR 2012 | AFM + DNB NEN-7510D

    https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure
  - Zoho EU Data Center Amsterdam, Netherlands

    The Zoho Data Center in the Netherlands has the following certifications: ISO 27001 ISO 22301 SOC 2 TYPE IIISO 50001 PCI DSSZoho EU Data Center Amsterdam, Niederlande

B.2. access and access control measures

Definition

Measures that ensure that

- data processing systems cannot be used by unauthorized persons,
- attempts to gain unauthorized access do not go unnoticed,
- the persons authorized to use the data processing systems can only access the data subject to their access authorization, and unauthorized reading, copying, modification is prevented,
- the attempt of unauthorized access does not go unnoticed.

B.2.1. Access authorizations

- Defined approval process, which employee has access to which personal data.
- Allocation and access authorizations are logged.
- Each employee receives a personalized user account.
- Each employee must identify himself at each log-in via a 2-factor authentication.
- There is a password parameter:
  - The password contains at least 8 characters,
  - Passwords contain upper and lower case letters, numbers and special characters,
  - Passwords must not be easy to guess (date of birth),
  - Trivial passwords (1111) must not be used,
  - Passwords that have already been used must not be used again.

- The system enforces compliance with the password requirement.
- In case of inactivity, the screen turns off after 5 minutes.
- If compromise is suspected, the password must be changed immediately using 2-factor authentication.
- Login attempts are limited and also remain locked until manually unlocked by IT.
- For remote access, employee identification is also done through 2-factor authentication.
- Login attempts for remote access are limited and also remain blocked until manually cancelled by IT.

B.3. Measures for securing paper documents, mobile data carriers and mobile devices

Definition

Measures that ensure the implementation of appropriate technical and organizational measures also on mobile data carriers and end devices as well as on paper documents.

B.3.1. Paper documents

- Confidential and secret information in paper form shall be disposed of exclusively via the shredder provided in the company (security level P4).

B.3.2. Mobile data carriers and mobile end device

- Data carriers are used for the exchange of data. Data carriers of unknown origin must not be used together with company hardware.
- Mobile data carriers used for data exchange, such as USB sticks, must be encrypted on the hard disk.
- The use of private mobile end devices is prohibited.
- The disposal of mobile end devices and data carriers is carried out by the IT department.

B.3.3. Maßnahmen zur sicheren Datenübertragung

Definition

Measures that ensure that

- Data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data media.
- Transportation of physical media containing personal data to a document destruction service provider is only carried out in closed containers and in closed vehicles so that no data can be lost.

B.3.4. Forwarding control

- E-mails are transmitted via TLS.
- Operation and use of an FTP server through which file sharing and secure or encrypted file transmission is ensured.

- Data media used for file sharing are encrypted.
- Keys or certificates are managed by in-house IT.

C. Measures to ensure availability

Definition

Measures to secure data (physical / logical) against accidental destruction or loss.

C.1. Server room

- The server room is an interior room without windows.
- The server room is protected by a fire-retardant solid wall access door.
- The server room is connected to the fire alarm control panel.
- The server room is equipped with both an extinguishing system (CO2 extinguisher and halon/ argon extinguishing system) and air conditioning.
- Uninterruptible power supply, which is additionally protected by a diesel generator and its functionality is tested regularly.

C.2. Backup and emergency concept, virus protection

- Documented backup concept.
- Regular testing of the backup concept.
- Execution and documentation of the backup check takes place at regular intervals but at least twice a month.
- The execution and documentation of the backup checks are carried out by the external service providers Microsoft Azure and Zoho.
- The regular creation of backups takes place on the online cloud storage of the aforementioned external service providers.
- The storage of the backups takes place in a separate section from the primary server.

C.2.1.1. Change- und Patchmanagement

- Documentation of change and patch management for which in-house IT is responsible.

C.2.1.2. emergency prevention concept

- Documentation of an emergency preparedness concept with precise action specifications.

C.3. Virus protection

- All servers and clients are provided with virus protection, which is constantly updated by the in-house IT department. As a matter of principle, no computers may be operated without up-to-date virus protection.

C.4. Network connection

- The entire network connection is operated by the in-house IT and is not redundantly connected to each other with regard to the individual locations.

D. Pseudonymization/encryption, Art. 32 (1) a DSGVO

Definition

Pseudonymization (Art. 32 Para. 1 lit. a, Art. 25 Para. 1 DSGVO) ensures that identification features of personal data are replaced by identifiers of specific or identifiable persons, insofar as this is necessary to protect the data subjects or is required from the perspective of data protection law, and therefore the assignment to the data subject is not possible without additional information. Consequently, data can no longer be assigned to a specific data subject without the addition of additional information. This additional information must be stored separately and be subject to appropriate technical and organizational measures.

D.1. Use of pseudonymization

- Where possible, data is processed pseudonymously.
- If data is analyzed as part of the commissioned processing, it is pseudonymized or anonymized in accordance with data protection requirements. Furthermore, pseudonymization of data in the overall process is ensured to the extent that only a unique, usually non-consecutive number is printed or encoded in the 1D or 2D barcode on scannable access badges of visitors and exhibitors ("badges"), which is only merged with the personal data of the respective visitor as part of the encrypted communication of the Scan2Lead front-end devices with the back-end systems.
- Assignment and storage of individual data is done in separate systems from each other.

D.2. Use of encryption

- Where possible, data shall be processed in encrypted form. This is to be assessed on a case-by-case and project-dependent basis.
- - Communication between the frontend devices of Scan2Lead users and the backend systems takes place exclusively using common encryption methods.

E. Procedure for reviewing, assessing and evaluating the measures taken - Art. 32(1)(b), (c), (d) GDPR

E.1. Conducting system audits

- System audits to verify the existing systems and whether they are functioning.
- If deviations or non-conformities are found, these are included in the risk assessment and appropriate countermeasures are initiated.
- Continuous review and documentation of the results.

E.1.1. Data protection management

- Appointment of a company data protection officer
- Commitment to data protection compliance in accordance with the GDPR
- Informing employees on the topics of data protection and data security through training and written explanations (appendix to the declaration of commitment)

- Conducting classroom training and e-learning (e.g., upon hiring) on data protection topics
- Conclusion of contracts for commissioned processing in accordance with Art. 28 DSGVO
- Passing on obligations from the written contract for commissioned processing to subcontractors
- Guidelines and checklists for commissioning service providers
- Control of the technical and organizational measures taken by the contractor
- Informing the client in the event of errors/irregularities in data processing
- Explanations and guidelines on data protection topics and requirements from the GDPR (e.g., dealing with data subject inquiries / procedure in the event of a "data breach," etc.).Bestellung eines betrieblichen Datenschutzbeauftragten

E.1.2. Documentation

- The measures taken are continuously reviewed and revised if necessary.