Technical and organisational measures for data security

Auerswald GmbH has taken the following technical and organisational measures for data security within the meaning of Art. 32 GDPR:

1. Confidentiality

1.1. Physical access control

Auerswald GmbH is spread across two sites in 38162 Cremlingen:

- "Hordorfer Straße 36" site:
  production, repair, purchasing, dispatch and the company's own training centre
- "Vor den Grashöfen 1" site:
  development, accounting, human resources, sales, marketing and product management

Access rules for employees

Both buildings are locked around the clock. Access is granted exclusively to employees of Auerswald GmbH via an electronic locking system that is managed by the IT and human resources departments. The issuing and administration of transponders follow a documented process both when an employee joins and when they leave. Access rights are granted on the "need-to-access" principle. Employees are given access only to the areas required for their work.

Access rules for visitors

- "Hordorfer Straße 36" site:

  Visitors are admitted only after the door has been opened by reception or an authorised person. Reception has visual contact with the entrance area and ensures that every visitor registers. Conversations with external persons take place exclusively in the designated meeting rooms.

  Participants in Auerswald Academy training courses may move only within the designated area of the training centre. Access to office and production areas is secured by the transponder system and is not permitted. Exceptions to this are factory tours, which are possible after prior registration and documentation.

– "Vor den Grashöfen 1" site:

  This site is generally not intended for visitors. In exceptional cases, a visit is possible after prior registration by telephone and collection in person at the entrance. Visitors must sign the visitors' book.

Security measures

Outside regular working hours, access to the buildings is possible only with an individual, employee-specific code in addition to the transponder. In addition, the entrance to the company premises on Hordorfer Straße is secured by an electronically controlled gate that can be opened only by transponder. The production, repair, dispatch and storage areas at the Hordorfer Straße site are additionally protected by an alarm system. All employees are trained in the use of the system.

1.2. System access control

Access to IT systems is possible only with a valid user authorisation. It is granted exclusively upon application by the respective manager or the human resources department and is implemented by administrators.

Authentication

Every user ID is unique. Initial passwords must be changed after the first login. The password policy of Auerswald GmbH provides for the following:

- minimum length: 12 characters
- use of upper and lower case letters, numbers and special characters
- lockout after three incorrect entries
- Passwords are stored in encrypted form. Systems enforce an automatic screen lock after 5 minutes of inactivity.

Network security

Remote access takes place exclusively via encrypted VPN connections. All server and client systems have up-to-date antivirus software and are protected by firewalls. An intrusion prevention system detects and prevents unauthorised access attempts.

All systems are regularly supplied with security updates and patches.

1.3. Data access control

Authorisations for IT systems and applications are set up exclusively by administrators and granted on the need-to-know principle. There is a role-based authorisation concept that ensures that employees can access only the data they need for their respective task. Project-related rights can be granted and revoked temporarily.

Data media and paper are destroyed by a certified service provider in accordance with DIN 66399. Employees are obliged to dispose of personal or confidential data exclusively in the security containers provided for this purpose.

The installation of unapproved software on IT systems is prohibited.

1.4. Separation of data

All IT systems used by Auerswald GmbH for customers are multi-client capable. The separation of data from different customers is ensured at all times.

1.5. Pseudonymisation and encryption

Administrative access to server systems generally takes place via encrypted connections.

In addition, data on server and client systems is stored on encrypted data media. Corresponding hard disk encryption systems are in use.

2. Integrity

2.1. Input control

The entry, modification and deletion of personal data processed by Auerswald GmbH on behalf of a controller is generally logged.

Employees are obliged always to work with their own accounts. User accounts may not be shared or used jointly with other persons.

2.2. Transfer control

Personal data processed on behalf of customers of Auerswald GmbH may be passed on only to the extent agreed with the customer or necessary for the provision of the contractual services for the customer.

All employees working on a customer project are instructed with regard to the permissible use of data and the arrangements for passing data on.

Where possible, data is transmitted to recipients only in encrypted form.

Employees of Auerswald GmbH are prohibited from using private data media in connection with customer projects.

Employees of Auerswald GmbH receive regular training on data protection topics. All employees have been obliged to treat personal data confidentially.

3. Availability and resilience

Data on server systems of Auerswald GmbH is backed up incrementally at least daily and in full weekly. The backup media are taken in encrypted form to a physically separate location.

The restoration of backups is tested regularly.

Auerswald GmbH has one server room at each of the two sites. Both server rooms are air-conditioned, are located above the water line and have an uninterruptible power supply (UPS) as well as fire alarm systems with suitable extinguishing systems. In addition, in the event of longer interruptions, a diesel generator takes over the power supply of the main server room located at the "Vor den Grashöfen 1" site.

All server systems are subject to monitoring that immediately triggers notifications to an administrator in the event of faults.

An emergency and restart plan is documented and tested regularly.

4. Procedure for regular review, assessment and evaluation

A data protection management system is implemented at Auerswald GmbH. It includes both a crisis response plan for data breaches and a process for reporting data protection breaches to the competent supervisory authority.

The policies within the data protection management system are evaluated and adjusted annually with regard to their effectiveness by the data protection and information security team.

It is ensured that data protection incidents are recognised by all employees and reported without delay to the data protection officer or, in their absence, to the data protection and information security team. The latter will investigate the incident immediately. Insofar as data processed on behalf of customers is affected, it is ensured that those customers are informed without delay of the nature and extent of the incident.

When processing data for its own purposes, if the conditions of Art. 33 GDPR are met, a report will be made to the supervisory authority within 72 hours of becoming aware of the incident.

4.1. Control of commissioned processing

Personal data is processed exclusively within the European Union.

An external data protection officer has been appointed for Auerswald GmbH. Before external service providers are engaged, a data processing agreement is concluded pursuant to Art. 28 GDPR. The service providers are checked in advance and monitored regularly.

4.2. Data protection by design and by default

The principles of data protection by design and by default are already taken into account when developing the software solutions of Auerswald GmbH. For example, multi-factor authentication can be activated and access can be controlled via a differentiated role and rights concept. A tamper-proof audit trail documents all changes to personal data and authorisations in a comprehensible manner.

Access rights are granted on the principle of data minimisation.