dedomind GmbH
Linzer Strasse 17, 4100 Ottensheim, Austria
info@dedomind.com | dedomind.com

Technical and organizational measures for data protection

1. Access control

Denial of access to processing facilities used for processing to unauthorized persons

1.1 *Structural measures*

- Locked entrance and interior doors
- Video surveillance

1.2 *Technical measures*

- Procedures for user login and logout
- Management of admin rights
- Password requirements/password safe

1.3 *Organizational measures*

- Visitors are not left unattended on the company premises
- Avoidance of paper files

2. Data carrier control

Prevention of unauthorized reading, copying, modification, or removal of data carriers

2.1 *Technical measures*

- Secure storage of storage media
- Data protection-compliant disposal of devices with storage media (e.g., printers)
- Data protection-compliant deletion and reuse of storage media (sticks)

2.2 *Organizational measures*

- Documentation of the issuance and use of mobile storage media (who has which USB stick or other storage medium? Numbering and assignment)
- Control over data transfer

3. Storage control

Prevention of unauthorized entry of personal data and unauthorized access, modification, and deletion of stored personal data

3.1 *Technical measures*

- Screen and computer lock when leaving the workplace
- User identification

3.2 *Organizational measures*

- Logging of the manner in which data is accessed

4. User control

Prevention of the use of automated processing systems with the aid of data transmission devices by unauthorized persons

4.1 Technical measures

- Firewall
- User identification
- Secure technical password specification
- Securing devices and networks

4.2 *Organizational measures*

- Determination of persons who have usage rights (responsibilities)
- Logging of users and activities
- Clear desk policy

5. Access control

Ensuring that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization

5.1 *Technical measures*

- User identification
- Encryption

5.2 *Organizational measures*

- Management and control of access authorizations
- Control of access (logging)

6. Transfer control

Ensuring that it is possible to check and determine to which locations personal data has been or can be transmitted or made available using data transmission facilities

6.1 *Technical measures*

- Logging of data transfers

7. Input control

Ensuring that it is possible to subsequently verify and determine which personal data has been entered into automated processing systems, at what time, and by whom.

7.1 *Technical measures*

- User identification
- Logging of the input, modification, and deletion of personal data.

7. *Organizational measures*

- Establishment of authorizations

8. Transport control

Preventing unauthorized reading, copying, modification, or deletion of data during the transmission of personal data and the transport of data carriers

8.1 *Technical measures*

- Encrypted transmission
- Access via encrypted VPNs
- Logging of data transmission
- Protection against malware (e.g., viruses)

9. Procedures for restoring systems

Ensuring that systems used can be restored in the event of a malfunction

9.1 *Technical measures*

- Data backups are performed at regular intervals
- Data backups are stored at off-site locations

10. Ensuring reliability and integrity

Ensuring that all functions of the system are available, that any malfunctions are reported, and that stored personal data cannot be damaged by system malfunctions

10.1 *Technical measures*

- Data backups are performed at regular intervals
- Use of virus scanners, firewalls, spam filters
- Use of electronic signatures

10.2 *Organizational measures*

- System monitoring of relevant hardware and software

Ottensheim, February 26, 2026