



MED SELECT
— HOLDING GMBH —

DATA PROTECTION & IT GUIDELINES

1. Purpose and Scope

These policies establish the requirements for the IT and data protection policies of the subsidiary company in order to ensure reliable, consistent, transparent and comparable reporting.



Contact

Med Select Holding GmbH:

Michael Husung

Email: m.husung@med-select.de

Tel.: +49 (0) 171 2119959

2. Principles

- The protection of personal data is a top priority.
- All employees are required to comply with legal requirements (in particular the GDPR and BDSG) and with internal data protection policies.
- IT systems must be designed to ensure data protection through privacy-friendly system design and default settings (Privacy by Design & by Default).

3. Access and User Administration

- Each employee is provided with an individual user account.
- Access rights are granted according to the need-to-know principle.
- Passwords must be changed regularly and chosen securely (at least 12 characters, upper- and lower-case letters, numbers and special characters).
- Sharing login credentials is prohibited.

4. Data Storage and Processing

- Personal data may only be collected, stored or processed if there is a legal basis for doing so (consent, contract, legal obligation, etc.).
- Data may only be stored for as long as they are required (storage limitation principle).
- Particularly sensitive data (e.g. health data) require additional protective measures.

5. E-mail and Internet Use

- Business e-mail must not be used for private purposes (unless specifically permitted).
- E-mails containing sensitive personal data must be encrypted.
- Attachments and links in e-mails from unknown senders must not be opened without verification.
- Visiting high-risk websites is prohibited.

6. Data Security and IT Infrastructure

- Security updates must be installed regularly on all devices.
- Antivirus software must be used and kept up to date.
- The IT department performs regular backups and checks that the data can be restored.
- Mobile devices (laptops, smartphones) must be protected by a PIN/password and, where applicable, by hard-drive encryption.

7. Data Retention and Destruction

- Files containing personal data must be stored in locked cabinets.
- Digital data must be securely deleted (e.g. using certified deletion software).
- Paper documents must be destroyed using a security-level P-4 shredder or higher.

8. Reporting Data Protection Incidents

- Data protection incidents (e.g. data breaches, lost devices) must be reported to the Data Protection Officer immediately.
- A 72-hour reporting deadline to the supervisory authority applies under Art. 33 GDPR.

9. Training and Awareness

- All employees must regularly complete data protection and IT security training.
- New employees must be instructed in these policies when they join.
- Refresher training should take place at least once a year.

10. Confidentiality Declaration

- All employees must sign a confidentiality declaration in accordance with Art. 5(1)(f) GDPR.
- The duty of confidentiality continues after the end of the employment relationship.

11. Confidentiality Declaration

- The Data Protection Officer is the first point of contact for all data protection matters.
- The IT department is responsible for implementing technical IT security measures.
- Managers are required to ensure compliance with these policies in their areas.



Thank You