



Fidelo Management Software

General Data Protection Regulation (GDPR)

Technical and organisational measures

Version: 1.3, 23.10.2025

General information

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. Enforcement date: 25 May 2018 – at which time those organizations in non-compliance may face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found on the website of the GDPR – <https://www.eugdpr.org/>.

Table of content

GENERAL INFORMATION	2
1. IT Security measurements	3
2. Physical security measures	3
3. Data protection security policy	3
4. Data breach management	4
5. Agreements	4
6. Training	4
7. Responsibilities	4
8. Data recovery and backups	4
9. Security and Data Protection Review	4
10. Data deletion	5
11. Resilience of the systems	5

1. IT Security measurements

Personal data is always protected by log-in and is only accessible to authorised employees. All access is logged.

All log-ins are protected by Intrusion Prevention Systems.

All data is secured during transmission using SSL/TLS encryption.

2. Physical security measures

Our servers are located in protected-access, high-security data centres.

Specifications:

- Individual access authorization
- Electronic access control systems and personnel monitor and guarantee that only authorized persons have access to the respective data centre
- Documentation of access authorizations
- Access documentation
- Authorized Guard Staff
- Role-based access rights for employees (administrators, assistants, cleaning staff, etc.)
- Visitor regulations
- Protection and restriction of access routes
- Transponder or key card-based locking system
- Video cameras as well as burglar and contact detectors monitor the outside of the building
- Access control system with chip cards
- Logging of user-relevant activities (login, logout, access denial, etc.)
- Demilitarized zones
- Infrastructure protection using burglar alarm systems
- Regular software updates
- User authentication required for system access and/or application access
- Automatic disabling of users following multiple failed logins
- Minimum password complexity required for passwords
- Encrypted storage of user passwords
- User login history
- Destruction of physical media according to DIN 32757
- Use of a shredder (minimum security level 3 according to DIN 32757)

The servers are continuously monitored via surveillance system. Our server administrators are informed of any unforeseen event.

3. Data protection security policy

We follow the European GDPR and the German BDSG.

Our employees are familiar with the basic rules and will promptly be informed about updates. They are trained to handle personal data.

4. Data breach management

Any data security breach must be dealt with and reported to those responsible as soon as it is made known. Any affected customers will then be notified about the breach.

5. Agreements

Our employees must confirm that they comply with the regulations set out in Art. 5, §1 (f) and Art. 32, §4 General Data Protection Regulation (GDPR).

6. Training

We give the employees a copy of the regulations and explain these in training sessions. Changes will be communicated to employees at least four weeks prior to coming into force.

7. Responsibilities

Responsible for security of personal information, data protection and training is Mark Koopmann, CEO (m.koopmann@fidelo.com)

8. Data recovery and backups

As required by law, recovery is initiated without delay (Article 32 (1) (c)) after an incident is detected.

A backup of the installations is created automatically overnight. At minimum 3 versions are kept on physically separate systems in a different location. The backups created are automatically checked to ensure the recovery process.

We also ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident as described in Art. 32 c).

To make sure the technical and organisational measures take effect we are testing, assessing and evaluating the effectiveness. We also provide a review of the testing process once per year which is described in Art. 32 c).

9. Security and Data Protection Review

The Data Protection Officer, who also fulfils the role of Head of IT Security, is responsible for conducting internal reviews of all security and data protection measures.

Reviews are performed annually and following any major system or infrastructure change.

Each review covers:

- access control and authentication procedures
- encryption and transmission security
- data storage and backup integrity
- incident response and breach management
- staff training and policy compliance

The review process follows a documented checklist to ensure objective assessment.

Results are recorded, signed off by senior management, and stored for a minimum of five years.

Although we do not hold external certifications (e.g., ISO 27001), internal processes are aligned with ISO 27001 control objectives and GDPR Article 32 requirements.

10. Data deletion

Our software provides tools within the application that enable users to delete and anonymize personal data, ensuring compliance with GDPR requirements. Users are responsible for the proper use of these tools to manage their data. Fidelo Software GmbH offers guidance on their use but is not responsible for individual data deletion actions carried out by users.

11. Resilience of the systems

Fidelo Software GmbH undertakes the measures to ensure the resilience of its IT systems. In principle, penetration tests of the client's IT systems are not part of the service provided by Fidelo Software GmbH, unless separate agreements have been made in the main contract.