



Data protection policy in accordance with the EU General Data Protection Regulation (GDPR)

Data protection policy

Goal of the data protection policy

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) but also to provide proof of compliance.

Preamble

Brief description of the company and motivation to comply with data protection.

Security policy and responsibilities in the company

- For a company, in addition to existing corporate objectives, the highest data protection goals are to be defined and documented. Data protection goals are based on data protection principles and must be individually modified for every company.
- Determination of roles and responsibilities (e.g. representatives of the company, operational data protection officers, coordinators or data protection team and operational managers)
- Commitment to continuous improvement of a data protection management system
- Training, sensitisation, and obligation of the employees

Legal framework in the company

- Industry-specific legal or conduct regulations for handling personal data
- Requirements of internal and external parties

- Applicable laws, possibly with special local regulations

Documentation

- Conducted internal and external inspections
- Data protection need: determination of protection need with regard to confidentiality, integrity and availability.

Existing technical and organisational measures (TOM)

Appropriate technical and organisational measures that must be implemented and substantiated, taking into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs.

The description of the implemented TOM can, for example, be based on Art. 32 GDPR:

- Pseudonymisation (Art. 32 (1) (a) of the GDPR; Art. 25 (1) of the GDPR)
- Encryption (Art. 32 (1) (a) of the GDPR)
- Confidentiality (Art. 32 (1) (b) of the GDPR)
 - Access Control
 - Entry Control
 - Authorisation Control
 - Separation Control
- Integrity (Art. 32 (1) (b) of the GDPR)
 - Transfer Control
 - Input Control
- Availability and Resilience (Art. 32 (1) (b) of the GDPR)
 - Availability Control
 - Resilience Control
- Recoverability (Art. 32 (1) (c) of the GDPR)
- Procedures for Regular Review, Assessment and Evaluation (Art. 32 (1) (d) of the GDPR; Art. 25 (1) of the GDPR)
 - Data-Protection-Management-System
 - Incident-Response-Management-System
 - Data Protection by Design and Default
 - Order Control