Updated: 2 September 2019

Data protection policy in accordance with the EU General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 201

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) and Data protection Act (DPA) 2018 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 the structure of ISO/IEC 27002, taking into account ISO/IEC 29151 (guidelines for the protection of personal data). The respective chapters should be substantiated by referencing the existing guidelines.

Examples of such guidelines include:

- Guideline for the rights of data subjects
- Access control
- Information classification (and handling thereof)
- Physical and environmental-related security for end users such as:
    - Permissible use of values
    - Guideline for information transfer based on the work environment and screen locks
    - Mobile devices and telecommuting
    - Restriction of software installation and use
- Data backup
- Information transfer
- Protection against malware
- Handling technical weak points
- Cryptographic measures
- Communication security
- Privacy and protection of personal information
- Supplier relationships: Noting regular inspection and evaluation of data processing, especially the efficacy of the implemented technical and organisational measures.

ST3 Architectural Tiles Limited, Unit 6 Monksbridge Trading Estate, Outgang Lane, Dinnington,
Sheffield, S25 3QZ. T +44 (0) 1909 561042 E info@st3tiles.co.uk