newclicks

Overview of technical and organizational measures

Appendix 1

Confidentiality

a) ACCESS CONTROL ((For buildings and rooms; on cabinets and shafts) Measures to prevent unauthorized persons from gaining access to data processing facilities where personal data are processed or used:

- Factory security service, gatekeepers, security personnel
- Access control system
  (e.g. ID card readers, locks, magnetic cards)
- Surveillance equipment
  (Alarm system, video, motion detectors on doors and windows)
- Key control and receipt at key issuance
- Secured doors, security locks, windows
- Control of cleaning and maintenance work
- Special access protection server rooms
  (electronic access control/logging)

b) ACCESS CONTROL/USAGE CONTROL
Log in to the system, prevent unauthorized boot-up and intrusion into the IT-system) Measures to prevent the use of data processing systems by unauthorized persons:

- Password management
  (at least 8-digit password, password complexity, regular change)
- Automatic locking, log-out
- Authorization rules/ terminals
- Special user menus
- Firewall, virus protection, DMZ
- Intrusion Detection/ Intrusion Prevention
- Backup of external interfaces (USP ports, CD/DVD drives)

c) ACCESS CONTROL

Measures to ensure that the persons authorized to use a data processing system can only access the data subject to their access rights and that personal data cannot be read, copied, altered or removed without authorization during processing, use and storage:

- ✔ Logging of accesses
- ✔ Differentiated authorizations (profiles, roles)
- ✔ Documentation of authorizations
- ✔ Storage of data media in lockable cabinets
- ✔ On-boarding/off-boarding process

d) SEPARATION CONTROL

Measures to ensure that personal data collected for different purposes and for different entities are processed separately.

e) PSEUDONYMIZATION AND ANONYMIZATION

(In the case of pseudonymization, the name or other identification feature is replaced by a pseudonym during anonymization, in order to exclude the establishment or to make it considerably more difficult to establish the identity of the person concerned without the need for additional information).

- ✔ use of a pseudonym for the name is possible
- ✔ The communication partner does not know the real identity,
  but the service provider does

Integrität

f) TRANSMISSION CONTROL AND ENCRYPTION

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and determine to which points personal data are to be transmitted by data transmission facilities:

- ✔ Encrypted communication/data transfer (https: VPN, SSL etc.)
- ✔ Password-protected transmission of documents

g) INPUT CONTROL (traceability, documentation)
Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and determine to which points personal data are to be transmitted by data transmission facilities:

- Access regulations/roles
- Logging of accesses
- 1-month storage

h) ENSURING AUTHENTICITY & INTEGRITY
(Protection against unauthorized or unlawful processing and against accidental loss, accidental destruction or accidental damage as well as unauthorized modification).

- Documentation of authorizations
- Encryption of data transmission
- Monitoring devices of the data processing systems

i) DATA PROTECTION MANAGEMENT
(Measures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures).

- Regular data protection audits
- Order control &unambiguous contract design
- Strict selection of service providers
- Pre-checks and follow-up checks
- Privacy-friendly presets
- Data Protection Officer

Availability and resilience

k) AVAILABILITY CONTROL
(traceability, documentation) Measures to ensure that personal data is protected against accidental destruction or loss, against technical malfunctions due to failure of the operating/application software, against negligent/intentional actions, against damaging software:

- Creation of redundancies
  (stock backup concept, backup copies, backups, data mirroring)
- Separate data storage
- Emergency concept/ emergency plan
- Uninterruptible Power Supply/ (UPS)
- Controlled shutdown of the emergency Monitoring systems
- Monitoring
- Automatic defense systems
- Regular PEN tests

Procedures for periodic review, assessment and evaluation

I) DATA PROTECTION MANAGEMENT
(Measures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures).

- Regular data protection audits
- Order control & unambiguous contract design
- Strict selection of service providers
- Pre-checks and follow-up checks
- Privacy-friendly presets
- Data Protection Officer

Rheinberg, 2026

Richard Zelzer   Andreas Feldmann

newclicks UG (haftungbeschränkt) & Co. KG