TECHNICAL AND ORGANIZATIONAL MEASURES LUWARE AG

CONFIDENTIALITY

- Access Control: Prevention of unauthorized access to data processing systems

Security locks; Chip card / transponder locking system; Door security (electric door closer, TV monitor); Alarm system; Intrusion detection system; Video surveillance; Visitors only when accompanied by an employee permitted; Verifiable key control; Locking of office doors in absence / outside working hours; Closing of windows in absence / outside working hours; Determination of authorized persons (employees and non-employees); Third party companies always under supervision; Visitor regulation; Security areas

- Access Control: Prevention of unauthorized system use

Use of encryption routines for files and data carriers; Access to wireless network encrypted (WLAN); Controlled destruction of data media; Password policy; Clean-desk-policy; User locked in case of repeated incorrect password input; Process when an employee joins; Process when an employee leaves; Procedures for data collection templates; Audit, voting and control systems; File organization guidelines (Attachment to project folders / shares / etc.);; Assignment and securing of identification keys; Non-disclosure agreements (all Employees sign a confidentiality agreement before beginning their work at Luware); Usernames / passwords for all data and programs; Differentiated access control; Locking of data terminals; Creation of a user master record per user; Use of up-to-date firewall; Use of up-to-date virus protection; Functional and/or timely limited use of terminals; Identification of a terminal on the IT system

- Access Control: User control; Prevention of unauthorized reading, copying, modification or removal within the system

Encryption of laptops; Administration of user rights by system administrators; Use of an up-to-date firewall; Video surveillance; Limitation of access time; Use of up-to-date virus protection; Reduced number of administrators (need-to-know basis); Implementation of additional account without administrator privileges; Verification of authorization; Restriction of free querying possibilities of databases (query language); Use of shredders; Use of service providers for file and data destruction; Data protection compliant deletion / rewriting before reuse of a data carrier; Use of personalized administrator accounts; Use of encryption routines for files and data carriers; Process in case of an employee's entry or leave; Regulation of access on a strict need-to-know basis; Limited access possibilities to databases and functions in accordance with the tasks of employees; IT systems with up-to-date firewalls

- Separation Control: Separated data processing for data which have been collected for different purposes

Separate databases; Separate tables within databases; Separate folder structures (order processing); Logically separated storage on different systems or data carriers; Client separation (purpose related); Separation of networks (physical / logical) by application (Production / Test / DMZ); Separation of productive and test system.

- Pseudonymization: for reasons of data minimization

Pseudonymization takes place at Luware where appropriate and possible on request in which case the processing of the personal data takes place in such a way that the data can no longer be assigned to a specific person without the need for additional information.

INTEGRITY

- Transfer Control / Transmission Control: Prevention of unauthorized reading, copying, modification or deletion during electronic transmission

Use of an up-to-date firewall; Use of up-to-date virus protection; Data protection compliant deletion / rewriting before reuse of data carriers; Use of shredders; Use of service providers for file and data destruction (if possible with certificate) including logging of destruction; Use of encryption routines for files and data media; Use of VPNs; Email Encryption on demand; Fixed disk storage; Authorized persons identification; Secure entrance to data center for deliveries; Separated locking of confidential media; Security

cabinets; Transfer of data in anonymous or pseudonymous ways

- Entry Control / Data Media Control / Storage Control: Determination if and by whom personal data is entered, modified and deleted

Traceability and logging of input; Modification and deletion of data by individual users; Use of electronic signature, procedural, program, and workflow organization; Assignment of rights for input; Change and deletion of data based on an authorization concept; Cloud Customers data storage on Microsoft Azure Cloud.

AVAILABILITY / CAPACITY / RECOVERABILITY

- Protection of accidental or intentional destruction or loss

Storage of data in a safe, separated location; Alarm notification in case of unauthorized access to server rooms; Fire protection measures; Emergency plan; Backup and recovery concept; Antivirus concept; Execution of regular backups; Design of measures for property security; Fire and smoke alarm systems; Devices for monitoring temperature and humidity in server rooms; Air conditioning; Fire extinguishers in front of server rooms; Power strips in server rooms; Server rooms not under sanitary facilities / near the central water supply; Mirroring of hard disks e.g. RAID procedure; Use of an up-to-date virus protection; Use of an up-to-date firewall; Service and maintenance contracts for software and hardware

REGULAR REVIEW, VALUATION AND ASSESSMENT

- Data Protection-, Incident-Response- and Processing Management

Data processing only under direction of the data controller (Data Processing Agreements in place where applicable); Verification of availability of required systems/ data carriers/ license keys etc. to ensure the rapid recovery of data and programs (disaster recovery scenarios); Regular data and program recoverability tests; Data backup scenarios - the respective application must also be available in the version status of the data backup to ensure recovery; Appointment of a data protection officer; early involvement of the data protection officer in new projects; Data protection organization in the company; Privacy policies; Processes to optimize data protection; Regular review of data protection standards; privacy by default; Obligation of secrecy by all employees and other third parties (if applicable); Training and instruction for employees

CERTIFICATIONS / AUDIT REPORTS

- ISO27001
- ISO9001
- SOC 2 Type 2 for security principles