Annex 1: Technical and Organizational Measures

Call for action	Legal requirement	Implementation in practice
Entry Control	Denying unauthorised persons access to data processing systems	The company building is guarded by a security service. All entrances to the building are under video surveillance. The main entrance is manned by a gatekeeper. All side entrances can only be opened via chip cards. The main entrance doors to the building are firmly locked outside operating hours. Third parties have no access to the premises. Building and office doors are alarmed. Visitors are received by the doorman and their registration is checked. An electronic locking system with different authorisation levels ensures that employees can only enter rooms for which they have been specifically authorised, in addition to the general areas. Server rooms can only be entered by authorised staff with chip cards. Entrances to rooms with increased security requirements are accessible via chip cards and special authorisations and are electronically recorded and monitored.
Access Control	Preventing the use of data processing equip-ment by unauthorised persons	All staff computers have virus protection. To gain access to data processing systems, staff must identify themselves with at least user ID & password. Screens are automatically locked after a short period of inactivity. Each staff member has their own user account with individual access rights. The number of login attempts is logged and after exceeding the maximum number of incorrect login attempts, the user account is locked. Unlocking is only possible by an administrator after authentication of the employee. After unlocking, the user is prompted to enter a personal password. Mobile work for employees is secured by VPN. All end devices and data carriers are encrypted, if possible. The company networks are secured by firewalls. The network segments are separated by a firewall. The firewall settings are checked regularly. A policy on the departure of employees (revocation of rights) and a password policy have been adopted.
Admission Control	Ensuring the use of a DP system and the stored data according to the authorisation	All access options and user roles are recorded in authorisation concepts and regulated analogously. All employees are bound to data secrecy.

		Certificates are issued for authentication and accesses are logged. In addition, protocols are used that include transport encryption.
Transfer Control/ Transmission Control	Data may only be transferred to authorised recipients	Transport encryption is used. Data records are identified by IDs rather than by plain names or other personal data. The principle of data minimisation is observed. A standardised process for destroying data media in a data protection-compliant manner is followed.
Plausibility check/ Transaction control	Ensuring traceability of (intentional and unintentional) data manipulations	Plausibility checks are carried out.
Order Control/ Contract Conformity Control	Ensuring the processing of data on behalf of the client in accordance with instructions	In order to protect personal data, contractors are carefully selected with regard to technical and organisational measures and corresponding order processing contracts are concluded. The company's own technical and organisational measures are reviewed on a regular basis. An external data protection officer is provided.
Availability Control	Securing data against accidental destruction or loss	Availability, rapid recoverability and protection against losses are ensured by uninterruptible power supply (UPS) with surge protection, RAID solutions and daily backups. All offices and server rooms are equipped with fire and smoke detection systems. An analysis of the server room situation has been carried out, server rooms are air-conditioned. Regular updates are carried out on all systems.
Data Segregation Control/Client Separation Control	Ensuring the separation of data collected for different purposes	Development/test and productive environments are separated from each other and data processing systems are separated from each other for specific purposes. Only those personal data are collected that are necessary for the respective purpose. During the development process of new software, it is already ensured that it is realised in a data protection-friendly manner.