Stay Open.

Technical and Organizational Measures

1.	Corporate measures of **access and data media control**, which prevent unauthorized persons from getting physical access to the information systems, the data processing device and the confidential files and data media	**Implemented mechanisms:** • key management / documentation of key distribution • door protection (electronic door-opener; biometric access control) • special server room protection • restricted areas **International standards** • ISO/IEC 27001:2013 certified, determined in No. 9.1 (Secure areas), 9.2 (Equipment security)

2.	Corporate security measures concerning **user control**, which prevent data processing systems from being used without authorization	**Implemented mechanisms:** • personal and individual user-log-in to the system resp. network • keyword policies (description of keyword parameter concerning complexity and interval of updating) • additional system-log-in for certain applications • automatic blocking of clients after a certain time lapse without user activity (password protected screen saver or automatic log-off) **International standards** • ISO/IEC 27001:2013 certified, determined in No. 11 (Access controls), 11.4 (Network access control) and 11.5 (Operating system access control); 12.3 (Cryptographic controls)
3.	Corporate measures of **access control**, which ensure that users entitled to use a data processing system can only access data to which they have a corresponding right of access	**Implemented mechanisms:** • administration of access and/or authorization rights as well as of system roles • groups • documentation of access rights • authorization routine • logging • regularly reviewing / auditing • encryption of notebooks, PCs and external hard drives • keyword identification for shell access **International standards** • ISO/IEC 27001:2013 certified, determined in No. 11 (Access controls); 10.1.3 (Segregation of duties); 8 (Human resources), 10.10 (Monitoring)

4.	Corporate security measures taken concerning **transmission and storage control**, to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport	**Implemented mechanisms:** • encryption of end user emails • encryption of notebooks, PCs and external hard drives • tunneled remote access (VPN) • logging • secured WLAN with WPA-enterprise • SSL-encryption for web-access • rules of destruction of data carriers **International standards** • ISO/IEC 27001:2013 certified, determined in No. 12.3 (Cryptographic Controls); 9.2.7 (Removal of property); 10.8 (Exchange of information)
5.	Corporate measures of **input control** that ensure to determine who has entered, modified or removed data from relevant systems	**Implemented mechanisms:** • access rights • logging within the system • security and/or logging software • “group based” and/or “function-related responsibilities” **International standards** • ISO/IEC 27001:2013 certified, determined in No. 12.2 (Correct processing in applications); 10.10 (Monitoring)

6.	Corporate measures guaranteeing that controller's personal data are processed just on behalf of the Controller and just within the Controller's instructions (**commission control**)	**Implemented mechanisms:** • regular training of employees with access rights • regular refresher courses • separate commitment of relevant employees on data protection compliance • regular data protection audits • determination of contact persons and responsibilities **International standards** • ISO/IEC 27001:2013 certified, determined in No. 12.5 (Security in development and support processes); 10.2 (Third party service delivery management); 6.2.3 (Addressing security in third party agreements)
7.	General corporate security measures concerning **availability control** and **reliability** against accidental loss or destruction of electronic data, files and data media	**Implemented mechanisms:** • back-up procedures • mirroring of servers and/or hard drives • uninterruptible electric power supply • storage procedures for back-ups (save deposit at a bank) • antivirus protection / firewall • emergency plans • air conditioning of server room **International standards:** • ISO/IEC 27001:2013 certified, determined in No. 10.5 (Information backup); 14 (Business continuity management)

8.	Measures in the Processor's systems which guarantee that data can be processed separately for separate purposes so that there is no unnecessary access to data which are stored for other purposes (**separation control**)	**Implemented mechanisms:** • separated systems • separated databases • access authorization • separation by access rights **International standards:** • ISO/IEC 27001:2013 certified, determined in No. 11 (Access controls); 10.1.3 (Segregation of duties); 10.10 (Monitoring)
9.	Corporate measures of **recoverability** guaranteeing that deployed relevant systems can be restored in case of failure	**Implemented mechanisms:** • back-up procedures • mirroring of servers and/or hard drives • storage procedures for back-ups (save deposit at a bank) • emergency plans **International standards:** • ISO/IEC 27001:2013 certified, determined in No. 10.5 (Information backup); 14 (Business continuity management)

10.	Corporate measures of **data integrity** to prevent stored personal data from damages caused by malfunctions of relevant systems	**Implemented mechanisms:** • access authorization • separation by access rights • separation by test and production environments • protection by firewalls • monitoring **International standards:** • ISO/IEC 27001:2013 certified, determined in No. 11 (Access controls); 10.1.3 (Segregation of duties); 10.10 (Monitoring)
11.	Corporate measures of **transport control**, which ensure that the privacy and integrity of data is protected when transmitting personal data when transporting data media	**Implemented mechanisms:** • encryption of end user emails • encryption of notebooks, PCs and external hard drives • tunneled remote access (VPN) • logging • secured WLAN with WPA-enterprise • SSL-encryption for web-access **International standards:** • ISO/IEC 27001:2013 certified, determined in No. 12.3 (Cryptographic Controls); 9.2.7 (Removal of property); 10.8 (Exchange of information)

12.	Corporate measures to ensure **encryption** and **pseudonymization** of data in order to ensure the integrity of personal data, as far as technically feasible.	**Implemented mechanisms:** • encryption of end user emails • encryption of notebooks, PCs and external hard drives • SSL-encryption for web-access • Adherence to the privacy policy that regulates storage and encryption • partial encryption of the storage **International standards:** • ISO/IEC 27001:2013 certified, determined in No. 12.3 (Cryptographic Controls); 9.2.7 (Removal of property); 10.8 (Exchange of information)