SCHEDULE C

TECHNICAL AND ORGANISATIONAL MEASURES

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1 Access control to premises and facilities (physical access control)

Access control to premises and facilities **Unauthorized access to premises and facilities must be prevented, whereas the term is to be understood spatially.**	**existent** **yes**
Electronic access code card / access transponders	X
Access authorization concept	X
Video surveillance	X
Key management	X
Visitor badges	X
Escorting of visitors‘ access by our own employees	X
Attendance records of visitor accesses	X
Scaled security areas and controlled access	X
Separately secured access to the data center	X
Storage of servers in locked rooms	X
Instruction for issuing keys	X

1.2 Access Control to Systems (Hardware access control)

Access control to systems **The intrusion of unauthorised persons into the data processing systems or their unauthorized use must be prevented.**	**existent** **yes**
Password protection of screens of workstations	X
Functional and/or time-limited assignment of user authorizations	X
Use of individual passwords	X
Automatic locking of user accounts after multiple incorrect password entries	X
Automatic password-protected screen locking after inactivity (screen saver)	X
Password policy with minimum requirements for password complexity:	
▪ Minimum of 8 characters / upper and lower case, special characters, numbers (of which at least 3 criteria)	X
▪ Prevention of trivial passwords (e.g. Dog1, Dog2, Dog3)	X
▪ Password history (no re-use of the last 5 passwords)	X
Procedure for the assignment of authorisations with the entry of employees	X
Procedure for revocation of authorisations due to department change of employees	X
Procedure for revocation of authorisations due to exit of employees	X
Obligation to confidentiality / data secrecy	X
Logging and regular evaluation of system usage	X
Controlled destruction of data carriers	X

1.3 Access control to data (software access control)

Access control to data **Unauthorised activities in data processing systems outside of assigned authorisations must be prevented.**	**existent** **yes**
Definition of access authorization, authorization concept	X
Restriction of free and uncontrolled query options for databases	X
Regular evaluation of logs (log files)	X
Partial access to data stocks and functions (Read, Write, Execute)	X
Use of appropriate security systems (software/hardware)?	
▪ Virus scanner	X
▪ Firewalls	X
▪ SPAM-Filter	X
Encrypted storage of data	
□ e.g. AES, RSA:	X

1.4 Separation Control

Separation control **Data collected for different purposes must also be processed separately.**	**existent** **yes**
Separation of customer data (multi-client capability of systems)	X
Authorization concept that takes into account a separate processing of data of different customers	X
Separation of development, test and production system	X

1.5 Pseudonymisation

(Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR) **The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without further information, provided that such additional information is kept separately and subject to appropriate technical and organisational measures**	**existent** **yes**
Measures:	X
PII vault is used to keep personal data	

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Control of transmission

Control of transmission **Aspects of the transfer (transmission) of personal data are to be regulated: electronic transfer, data transport as well as their control.**	**existent** **yes**
What is the mode of transmission of data between Controller and third parties?	
▪ Data exchange via https connection	X
▪ Other mode of transmission:	X
□ Encryption algorithm used:	X

- Hashes are added with a “Salt“ or “Pepper“	X
Secured entrance for supply and delivery	X
Documented management of data carriers, inventory control	X
Definition of the areas in which data carriers are stored	X
Encryption of data carriers with confidential data	X
Encryption of laptop hard disks	X
Encryption of mobile data carrier	X
Controlled destruction of data:	X
Data carrier disposal – Secure deletion of data carriers:	
▪ Physical destruction (e.g. shredder with particle cut - 1000 mm² max.)	X
▪ Others: e.g. overwriting of tapes and hard drives	X
Backup copies of data carriers that will have to be transferred	X
Documentation of the bodies to which transmissions are planned and the means of transmission	X
Packaging and shipping instructions, encrypted email dispatch	X
Control of completeness and correctness	X

2.2 Entry control

Entry control **Traceability and documentation of data administration and maintenance must be guaranteed.**	**existent** **yes**
Definition of user authorisations (profiles)	X
Differentiated user authorisations:	X
Read, modify, delete	X
Partial access to data or functions	X
Logging of entries / deletions	X
Log analysis system	X
Log concept going beyond OS standard	X
Dedicated log server	X
Control of access authorisations to log servers (log admin)	X

3. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

3.1 Availability control

Availability control The data must be protected against accidental destruction or loss.	existent yes
Data protection and backup concept	X
Carrying out data protection and backup concept.	X
Restriction of access to server rooms to authorised personnel	X
Fire alarm systems in server rooms	X
Smoke detectors in server rooms	X
Air-conditioned server rooms	X
Lightning / overvoltage protection	X
Water sensors in server rooms	X
Keep backup systems in separate rooms and fire compartment	X

Ensure technical readability of backup storage media for the future	X
Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)	X
CO^2 fire extinguishers in the immediate vicinity of the server rooms	X
Emergency plan (e.g. water, fire, explosion, threat of attacks, crash, earthquake)	X
Observation of the influence of adjacent buildings	X
Vulnerability analysis (terrain protection, building protection, intrusion into computers, computer networks)	X
Storage of data in data storage cabinets, safes	X
UPS system (uninterruptible power supply)	X
Power generator	X

3.2 Resistance and reliability control

Resistance and reliability control Systems must be able to cope with risk-related changes and must be tolerant and able to compensate disruptions.	existent yes
Alternative data centers available (Hot- or Cold-Stand-by?): **Cold**	X
Redundant power supply	X
Redundant UPS system	X
Redundant power generators	X
Redundant air conditioning	X
Redundant fire fighting	X
Hard disk mirroring	X
Computer Emergency Response Team (CERT)	X
Loadbalancer	X
Data storage on RAID systems (RAID 1 and higher)	X
Delimitation of critical components	X
Performance of penetration tests	X
System hardening (deactivation of non-required components)	X
Immediate and regular activation of available software and firmware updates	
▪ Identification of the different devices that make up the network and identification of their hardware version as well as their current software and firmware versions.	X
▪ Communication channel with manufacturers to stay up-to-date on any new updates and patches released for the devices owned.	X
▪ Definition of time periods in which the updates shall be implemented (e.g. periods of lower operations, maintenance times, etc.)	X
▪ Use of redundant systems to maintain operations while main devices are being updated.	X
▪ Progressive deployment of updates / patches to detect any issues early without affecting multiple devices.	X
▪ Specify a testing period to verify the correct implementation of the update and ensure that operations continue to run smoothly with the new updates.	X

Security is included as a main consideration during the design phase of the systems.	
▪ Definition of security measures to protect and validate communication between system components.	X
▪ Limitation of authorizations on a need-to-know basis.	X
▪ External contractors (service providers) and maintenance personnel must have a specific access, which must only be active during the intervention and remain disabled the rest of the time.	X
Periodic security training and awareness campaign within the organisation	
▪ Awareness campaigns to inform users of the security concepts of specific systems and traditional IT systems	X
▪ Specific security training to teach how to apply security measures and behaviours on the daily processes with the least impact possible.	X
Take out cyber-insurance	
▪ Identification of the devices, assets, and network systems within the organisation's infrastructure.	X
▪ Carrying out a risk analysis considering all these systems, devices and assets identified to determine the threats they are exposed to, their likelihood and impact.	X

4. Procedures for a regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

4.1 Control procedures

Control procedures **A procedure is to be implemented for regularly testing, assessing and evaluating the effectiveness of the data security measures.**	**existent yes**
Records of processing activities are reviewed and at least updated annually (where applicable).	x
Notification of new/changed data processing procedures to the Data Protection Officer.	x
Notification of new/changed data processing procedures to the IT Security Officer.	x
Processes for reporting new/changed procedures are documented.	x
Security measures are subject to regular internal audits	x
In the event of a negative outcome of the above-mentioned review, the security measures are adjusted, renewed and implemented in line with the risks involved.	x

4.2 Control of instructions

Control of instructions **It must be ensured that commissioned data processing by service providers (subcontractors) is only processed in accordance with the instructions of the Processor.**	**existent yes**
Contracts according to the requirements of Art. 28 GDPR	x

Centralized registration of commissioned service providers (contract management)	X