Appendix 2: Technical and organizational measures & subcontractors

Part 1: Pseudonymization

If applicable, please provide information on the pseudonymization techniques used by the data processor. If this is not applicable, please leave blank. Pseudonymization is the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separate.

Measure	YES/NO If Yes, please check the box or leave blank if unclear or not applicable.	
The personal data processed are pseudonymized (**please specify**):	□	....

Part 2: Encryption

If applicable, please provide information on the encryption techniques used by the data processor. This refers to any measures used to convert readable data into an encrypted version using an encryption key. Not all of the information below may apply, so please select only what is relevant to the processing activity.

Measure	YES/NO	
Virtual environments are encrypted (e. g. B. Citrix connections)	□	
VPN connection (IP-sec)	□	
Emails are sent encrypted. All Attachments are encrypted.	□	
Data exchange via an https connection	□	
Data carriers are encrypted	□	
Laptop hard drives are encrypted	□	
Mobile storage devices (e.g., USB stick) are used encrypted	□	
Hash function used (hashes are salted)	□	
Other algorithms/standards used **(please specify frame):**	□	....

Part 3: Confidentiality

a. Physical access controls

If applicable, please provide information about the physical access controls that the data processor uses. Physical access controls are restrictions on premises, buildings, rooms, and physical IT assets to prevent unauthorized access to data.

Measure	YES/NO
Doors, gates and windows are to be kept outside the Opening hours closed	□
Visitors are registered and on the premises □ accompanies	
The distribution of key and/or Magnetic cards are regulated and monitored	□
There are security personnel on site	□
There is video surveillance on the premises □	

There are alarms in the premises	□	
Servers are installed in a separate, stored in locked area	□	
Data backups are located in a separate, closed area	□	
Other (**please specify**):	□	....

b. Virtual access controls

Please provide details of any virtual access controls used by the data processor, if applicable. Virtual access controls are restrictions within systems that prevent unauthorized access to data.

Measure	**YES/NO**	
Devices are password protected	□	
User authorizations are, if necessary required and/or temporary	□	
Individual secure passwords become used	□	
Devices are switched off after failed Password attempts locked	□	
Automatic screensaver locks on Devices (after a certain time)	□	
Depending on their role, employees receive Access rights	□	
Access rights are changed when an employee leaves or changes roles System logs are	□	
in place (including file accesses and deletions).	□	
Virus scanners are in use	□	
Firewalls	□	
SPAM filter	□	
Intrusion protection (IPS) and Intruder detection (IDS)	□	
Other (**please specify**):	□	....

c. Separation controls

If applicable, please provide information on the separation controls used by the data processor. Segregation controls ensure the separation of personal data from other personal data that has a different purpose or originates from a different source (e.g., from another customer).

Measure	**YES/NO**	
Separation of customers (multi-client system)	□	
File separation in databases	□	
Virtual data separation (e.g., on the basis of the customer or client ID)	□	
Separation of functions	□	
Separation of development, test and productive Systems	□	
Other (**please specify**):	□	....

....
....

Part 4: Integrity

a. Transmission controls

If applicable, please provide information on the transmission controls used by the data processor. Transmission controls ensure the secure transmission, transfer, routing, and storage of data.

Measure	YES/NO
Inventory control of data carriers	□
Protocols for making copies of Data	□
Records of facilities to which Transfers are made	□
Packaging and shipping instructions for Data carrier	□
Other (**please specify**):	□

....
....
....
....

b. Incoming inspections

If applicable, please provide information on the input controls used by the data processor. Input controls are checks on whether and by whom personal data has been entered, modified or removed (deleted).

Measure	YES/NO
Are all data labeled?	□
User permissions are defined	□
Field access to databases	□
Partial access to the databases	□
Protocol Analysis System	□
Dedicated protocol server	□
Organizational determination of Input responsibilities	□
Access authorization for log server becomes controlled	□
Other (**please specify**):	□

....
....
....
....

c. Destruction controls

If applicable, please provide information on the destruction controls used by the data processor. Destruction controls are measures that ensure that security is maintained even when personal data is deleted or equipment is destroyed.

Measure	YES/NO
Virtual destruction of data (complete Overwrite etc.)	□
Physical destruction of data carriers (shredded)	□
Safe paper disposal (shredding)	□

Storage of waste in sealed containers before final destruction	□	
The data destruction systems used for the Service providers are reviewed	□	
Other (**please specify**):	□	....

Part 5: Availability

If applicable, please provide information on the availability measures taken by the data processor. Availability refers to the measures used to prevent and detect problems related to the continuous and successful provision of access to the personal data.

Measure	**YES/NO**	
Backups are created hourly or daily	□	
Backups are created weekly	□	
Recovery is tested frequently	□	
Server rooms are equipped with fire alarms and Smoke detectors equipped	□	
Server rooms are air-conditioned	□	
Protection against overvoltages is implemented	□	
Server rooms have water sensors	□	
Backups are performed separately from the main server before Place saved	□	
Backups are sent separately from the main server to stored at an external location.	□	
The future readability of the backup media is guaranteed.	□	
Power generator is installed	□	
Other (**please specify**):	□	....

Part 6: Resilience

If applicable, please provide details of the resilience measures employed by the data processor. Resilience refers to the measures taken to recover or restore from an incident that affects the provision of and access to personal data.

Measure	**YES/NO**	
Redundant power supply is available	□	
Redundant UPS system	□	
Redundant air conditioners	□	
Redundant fire extinguishing system	□	
Hard disks are mirrored	□	
Data storage on RAID systems	□	
Software and firmware updates are Regularly installed	□	
Other (**please specify**):	□	....

Part 7: Effectiveness

Please provide details of the effectiveness measures applied by the data processor, if applicable. Effectiveness refers to the regular and effective testing, evaluation or assessment of all of the above measures to ensure that they are successful. Such effectiveness measures may, for example, be performed internally or externally.

Measure	**YES/NO**
Internal record of the processes is created and monitors	□
The Data Protection Officer (DPO) shall be formally appointed	□
The IT security officer or the DPO are informed about changes in the processing informs.	□
Internal audits are carried out (at least yearly)	□
Privacy-friendly default settings are Always selected	□
External audits are carried out (at least yearly)	□
There is a formal certification (state...)	□
Audit recommendations are implemented	□
The service providers are regularly (at least annually) reviewed.	□
Clear procedures for responding to Data breaches are present	□

Other (**please specify**): □ ....
....
....
....

Subcontractor		
Name / Company	**Function**	**Seat / Address**

Name exhibitor	
Position	
Company name	