TECHNICAL AND ORGANIZATIONAL MEASURES

Below, the Service Provider will positively indicate, e.g. ☑, or otherwise state, the applicable technical and organizational security measures within each section that have been applied to the Processing of Protected Data associated with this agreement.

1. **Confidentiality** (Article 32 (1)(a) and (b) GDPR)
   Aim: To prevent unauthorized access or disclosure of protected data to individuals, entities or Processes.

- Physical Access Control - No unauthorised access to Data Processing Facilities, e.g.:
  - ✓Use of magnetic or chip cards
  - ✓ Keys
  - ☐ Electronic door openers
  - ☐ Facility security services and/or entrance security staff
  - ✓ Alarm systems
  - ✓ Video/CCTV Systems
  - ☐ Other (Specify below)

- Electronic Access Control - No unauthorised use of the Data Processing and Data Storage Systems, e.g.:
  - ✓ Firewall,
  - ✓ Use of (secure) passwords
  - ☐ Automatic blocking/locking mechanisms
  - ☐ Two-factor authentication
  - ✓ Encryption of data carriers/storage media
  - ☐ Other (Specify below)

- Internal Access Control (permissions for user rights of access to and amendment of data) - No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g.:
  - ☐ Rights authorisation concept
  - ✓ Need-based rights of access / role based access control
  - ✓ Logging of system access events
  - ☐ Other (Specify below)

- Isolation Control - The isolated Processing of data e.g.:
  - ☐ Multiple tenant/client support
  - ☐ Sandboxing
  - ☐ Other (Specify below)

- Pseudonymisation - The Processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.
  - ☐ Pseudonymisation
  - ☐ Anonymization
  - ☐ Scrambling
  - ☐ Masking
  - ☐ Blurring
  - ✓ Other (Specify below)

KxArchiver add-on

2. Integrity (Article 32 (1)(b) GDPR)
Aim: To provide assurance of consistency, accuracy and trustworthiness of protected data.

- Data Transfer Control - No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.:
  - ✓ Certificate based controls, (HTTPS, FTPS etc.)
  - ✓ Use of encryption
  - ☐ Virtual Private Networks (VPN)
  - ☐ Electronic/digital signature
  - ☐ Checksums
  - ☐ Other (Specify below)

- Data Entry Control - Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.:
  - ☐ Use of Logging,
  - ☐ Document Management,
  - ☐ Quality control,
  - ☐ Change management
  - ☐ Other (Specify below)

- Data Integrity Control - Awareness or control of changes to data.: e.g.:
  - ☐ File integrity monitoring
  - ☐ Rights management
  - ☐ Value limit
  - ☐ Completeness
  - ☐ Validation
  - ☐ Entity
  - ☐ Other (Specify below)

3. **Availability and Resilience** (Article 32 (1)(b) GDPR)
Aim: To ensure that information is accessible to authorized individuals, entities, or Processes when needed.

- Availability Control, e.g.:
  - ✓ Backup Strategy (online/offline; on-site/off-site)
  - ☐ Capacity plans
  - ✓ Uninterruptible Power Supply (UPS)
  - ✓ Virus protection
  - ✓ Reporting procedures
  - ✓ Contingency planning
  - ☐ Other (Specify below)

- Ability for timely recovery (Article 32 (1)(c) GDPR); e.g.:
  - ✓ Use of backup strategy – recovery time objectives, recovery point objectives
  - ✓ Disaster recovery plans
  - ☐ Other (Specify below)

- Architectural Control; To reduce the possibility of loss of service through architectural/structural design e.g.:
  - ✓ High availability designs
  - ✓ Load balancing
  - ☐ Redundancy
  - ✓ Failover
  - ☐ Raid configurations
  - ✓ Software update/upgrade Processes
  - ✓ Patch management
  - ☐ Other (Specify below)

4. **Effectiveness - Procedures for regular testing, assessment and evaluation** (Article 32 (1)(d) GDPR)

- Data Protection Management, e.g.:
  - ☐ Use of data register
  - ☐ Data inventory
  - ✓ User awareness training
  - ☐ Other (Specify below)

- Data Privacy Impact Assessments, e.g.:
  - ✓ Continued use of Privacy Impact Assessments
  - ✓ General risk assessments
  - ☐ Other (Specify below)

- Incident Response Management; e.g.:
  - ✓ Use of the corporate Incident handling procedure
  - ☐ Use of industry standard security incident handling procedures
  - ☐ Other (Specify below)

- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR); e.g.:
  - ☐ Pseudonymisation
  - ☐ Data minimization
  - ☐ Data segregation
  - ☐ Role base access controls
  - ☐ Encryption at rest
  - ☐ Other (Specify below)

- Order or Contract Control - No third party data Processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.:
  - ✓ Clear and unambiguous contractual arrangements
  - ☐ Formalised Order Management
  - ✓ Due diligence in selection of the Sub-Processor,
  - ☐ Duty of pre-evaluation
  - ☐ Duty of protection assurance
  - ☐ Supervisory follow-up checks
  - ☐ Other (Specify below)