ANNEX 1 - TECHNICAL AND ORGANISATIONAL MEASURES

CONFIDENTIALITY

- **Access control I:** Protection against unauthorised access to data processing facilities; Secured housing within the EU (Frankfurt); Data centre operator & location ISO27001:2013 and ISO9001 certified.
- **Access control II**: passwords (including corresponding policy); automatic locking mechanisms; no physical access to the hardware;
- **Access control III**: Standard authorisation profiles on a "need to know basis"; standard process for authorisation allocation; logging of accesses; periodic review of allocated authorisations;
- **Separation control:** Dedicated virtual server per Client / project; dedicated user accounts & passwords, extensive authorisation system; separate, databases;
- **Pseudonymisation:** guest/customer records are identified via UUIDs; IP addresses are temporarily (until the end of the project) stored separately & encrypted to analyse security incidents

INTEGRITY

- **Transfer control**: all incoming and outgoing connections are encrypted; logging of access; more sensitive data is additionally stored in encrypted form;
- **Input control**: logging; versioning; hourly backups;

AVAILABILITY AND RESILIENCE

- **Availability control**: Hourly off-site backups; uninterruptible power supply (UPS); data centre operator & location ISO27001:2013 and ISO9001 certified; hardware RAID; intrusion prevention system (IPS), permission system to prevent unauthorised applications from running; anti-virus programs on servers & Clients (Contractor staff).
- Rapid **recoverability** through hourly backups & versioning
- **Short deletion periods**: Both for data itself and metadata such as log files, etc., at the latest at the end of the agreement.

PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

- **Principles:** Data protection is the task of the entire company; data protection-friendly technologies are used; IT security must be state of the art
- **Data protection management:** Processing activities carried out are documented in a uniform and verifiable manner; instructions from & activities carried out for Clients in the context of commissioned processing are documented on a Client-specific basis.
- **Incident response management: There are** internal guidelines and processes for data protection that are expanded or supplemented as needed or as conditions change.
- **Data protection-friendly default settings:** Appropriate technical and organisational measures are taken for the respective processing purpose, which are assured to each Client as part of the agreement of a commissioned processing. Examples: New objects in the authorisation and access management have no rights in the system and are initially not allowed to see any data content. Evaluation results and lists can only be viewed by authorised persons.
- **Contract control:** No commissioned data processing within the meaning of Art 28 DS-GVO without corresponding instructions from the Client; obligation of the Contractor's employees to maintain data secrecy; appointment of a data protection officer; appointment of a data protection coordinator;
- Just in the process of ISO/IEC 27001:2017 & ISO/IEC 27018:2014 certification; regular staff training;