European Capital of Democracy
Data Security Guidelines

ECoD gemeinnützige GmbH (ECoD NPO) shall take technical and organisational measures to ensure data security and provide a secure cloud environment for the work on the required documents.

The undersigned declares to only use IT equipment (including mobile devices, such as laptops, tablets and smartphones)

- with a current updated version of operating system and other software
- with a current updated version of antivirus software
- where access to the the accounts being used to access the equipment is secured with a password that is only known to the authorised user
- where drive encryption features are activated if data is being stored on a laptop or removable device

Physical security is to be maintained if the location where the IT equipment is located is accessible to third persons. IT equipment must be locked (physically or using software functionality) if the authorised user leaves the location where the equipment is being used (e.g. by engaging screen locking functionality or keeping mobile devices in locked containers). Physical security must also be maintained for paper documents and other data carriers. The undersigned undertakes to keep paper documents and data carriers secure to avoid access by unauthorised persons, and will securely destroy paper documents and securely delete all information received from ECoD NPO after provision of the services.

Any information provided by ECoD NPO to the undersigned may only be used in line with the purpose for which it has been provided by ECoD NPO. Any use for other purposes - in particular the own purposes of the undersigned or its authorised persons – is strictly prohibited and may violate Data Protection Laws.

Furthermore, ECoD NPO and the undersigned shall ensure compliance with the GDPR and the Austrian Data Protection Act. Notwithstanding the above, ECoD NPO is the responsible party under Data Protection Laws. Data Processing Agreements (see separate document) shall be laid out and entered into if need be as required by Data Protection Laws.

APPENDIX – TECHNICAL AND ORGANISATIONAL MEASURES

Please tick the existing technical and organisational measures.

1. CONFIDENTIALITY

Entry control **Avoidance of unauthorised entry to data processing facilities by:**	
☐ Key	☐ Magnet or chip cards
☐ Electric door opener	☐ Doorman
☐ Security personnel	☐ Alarm system
☐ Video system	☐ Burglary-restraining windows and/or safety doors
☐ Registration at reception desk and identity check	☐ Follow-up checks on visitors to the premises
☐ Use of visitor or staff card/ID	☐ Other(s):
Access control **Avoidance of unauthorized system usage through:**	
☐ Password (including suitable policies)	☐ Encryption of data carriers
☐ Automated locking mechanism	☐ Other(s):
☐ Two-factor authentication	
Access control **Avoidance of unauthorized reading, copying, changing or deleting within the system by means of:**	
☐ Standard correction profile on a “need to know basis”	☐ Standard process for assigning authorisations
☐ Logging of access	☐ Safe storage of data carriers
☐ Regular checks of the assigned authorisations and of administrative user accounts in particular	☐ Privacy-compliant reuse of data carriers
☐ Privacy-compliant disposal of data carriers that are no longer needed	☐ Clear-desk/clear-screen policy
☐ Other(s):	
Pseudonymization	
If possible for the data processing operation, the primary identifiers are removed from within the data processing operation and saved elsewhere.	
☐ Yes	☐ No
Data classification scheme	
Based on legal obligations or self-assessment (secret/confidential/internal/public).	
☐ Yes	☐ No

2. DATA INTEGRITY

Prevention of (accidental) destruction of, (accidental) damage to, (accidental) loss of, or (accidental) changes to personal data.

Control of data transfer **No unauthorised reading, copying, changing or deleting during electronic transfer or transport by way of:**	
☐ Encryption of data carriers	☐ Encryption of data files
☐ Virtual private networks (VPN)	☐ Electronic signatures
☐ Other(s):	

Data entry control Determination of whether and by whom personal data has been entered into the data processing system, changed or deleted by means of:	
☐ Logging	☐ Document management
☐ Other(s):	

3. AVAILABILITY AND RESILIENCE

Availability control Protection against wilful destruction (negligent and/or wilful) or loss by means of:	
☐ Back-up strategy (online/offline; on-site/ off-site)	☐ Uninterrupted power supply (UPS, diesel generator)
☐ Virus protection	☐ Firewall
☐ Reporting channels and emergency procedures	☐ Security checks with regard to infrastructure and application
☐ Multi-level back-up approach with encrypted outsourcing of back-ups in a data centre at a different location.	☐ Standard procedures for staff changes
☐ Other(s):	
Rapid recoverability	
☐ Yes	☐ No

4. PROCEDURES FOR REGULAR TESTING, ASSESSING AND EVALUATING

Data protection management, including regular employee training:	
☐ Yes	☐ No
Incident response management:	
☐ Yes	☐ No
Data protection by design:	
☐ Yes	☐ No
Data processing control **No data processing in the sense of Art. 28 GDPR without specific instruction by the ECoD NPO by means of:**	
☐ Definitive contract design	☐ Formalized project management
☐ Strict selection of data processors (ISO-certified, ISMS)	☐ Due diligence
☐ Follow-up checks	☐ Other(s):

_____	_____
Place and Date	Place and Date
_____	_____
[insert name]	Representative of ECoD NPO