Annex No. 2. – Minimal security measures

1. Monitoring of access control

The Data Processor shall prevent unauthorized access to the systems where the Personal Data are being processed („**Data Processing Systems**"). The Data Processor therefore applies at least the following measures in datacenters where its infrastructure is hosted as well as its premises:

- Access control system (ID reader, magnetic cards, chip cards, biometric scanner)
- Door keys and key owners
- Audited key distribution
- Door-closing systems (monitored electronic closing systems)
- 24/7 Security personnel (in datacenters only)
- Physical security equipment (alarm systems, video/CCTV monitoring)

2. Entry monitoring

The Data Processor shall prevent that unauthorized parties may use or access the Data Processing Systems. The Data Processor therefore applies at least the following measures on its production systems, test environments and collaboration systems.

- Use of passwords (including special characters, minimal length, change of password)
- Use of two-factor authentication on systems whereas this solution is reasonable to use (front-ends)
- Session timeouts

3. Monitor of access rights:

The Data Processor shall guarantee that all persons using the Data Processing Systems to access Personal Data have special access permits regarding the Personal Data and that the Personal Data cannot be read, copied, altered or erased without permit. The Data Processor therefore applies at least the following measures (please indicate the relevant).

- Audited user provisioning
- Special access rights
- Access reports (logs)
- Monitoring of access
- Deprovisioning users
- In case of termination of the employment/contract relationship of the user deleting/withdrawing access rights are considered appropriate and shall include the following:

1.1 a) withdrawing all accessing rights to the IT systems;

1.2 b) disabling user accounts, wiping (5220.22-m where applicable) mobile devices used to access Personal Data;

1.3 c) taking back IT devices (e.g. laptop) used to control Personal Data;

1.4 d) withdrawing physical access rights;

1.5 e) taking back and recycling identification access cards.

1.6

4. Monitoring of users:

The Data Processor prevents unauthorized use of the Data Processing Systems. The Data Processor therefore applies at least the following measures (please indicate the relevant).

- Users shall be identified when added in order verify that they are who they claim to be;

- Binding agreement(s) concluded with the users that include among others confidentiality obligations and the obligation to comply with IT and security policies;
- Use of passwords (strong password policy) and identification keys (e.g. SSH keys, certificate authentication)
- Users may access different resources from specific locations. (enforced by privileges and packet filters)

5. Monitoring of data medium

The Data Processor prevents unauthorized reading, copying, altering or erasing of the data medium. The Data Processor therefore applies at least the following measures (please indicate the relevant).

- Prohibition of unauthorized cloud services
- Special access rights
- Automatic data consistency check (by design)

6. Monitoring of data transfer:

The Data Processor ensures that the Personal Data cannot be read, copied, altered or erased without authorization during electronic data transfer and that the above cannot be executed when copying, storing or transferring on data medium. The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Encryption (HTTPS/SSL)
- Encrypted VPN access for authorized users
- Electronic signatures whereas it is applicable
- AAA (Authentication, Authorization and Accounting)
- Packet filters

7. Monitoring of data recording (input control)

The Data Processor ensures that the identity of the persons involved with the Data Processing Systems and the schedule of processing Personal Data may be verified (input control). The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Logging and reporting systems
- Input sanitization

8. Monitoring of data storage:

The Data Processor prevents access to Personal Data by unauthorized parties and the unauthorized viewing, altering or erasing of stored Personal Data (monitoring of storage). The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Monitoring of access
- Audited access to data storage systems

9. Monitoring the execution of instructions:

The Data Processor ensures that Personal Data may only be processed in compliance with the instructions of the Data Controller. The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Audited online communication (logged, monitored, checked if requested)
- Monitoring the execution of instructions
- Regular internal monitoring and documentation by the Data Processor in order to confirm compliance with the instructions and the rules of executing instructions

10. Monitoring of the separation of competencies:

The Data Processor ensures that the Personal Data controlled for different purposes (if any) are being processed separately. The Data Processor therefore applies at least the following measures (please indicate the relevant):

- In case of multiple data controlling purposes the separation of the processed Personal Data by data controlling purposes
- Handling different purpose of data on separated logical environments

11. Monitoring of documentation:

The Data Processor ensures that the Data Controller may review the documentation of all significant processing steps of the Data Processing System and follow the individual steps of processing Personal Data. The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Documentation of data processing activities
- Reports or the excerpts of the reports of independent bodies (e.g. auditors, data protection officers, IT security department, data protection controllers, quality controllers)
- Approved codes of conduct pursuant to Article 40 of the GDPR
- Approved certification pursuant to Article 42 of the GDPR

12. Recovery monitoring:

The Data Processor ensures that the used Data Processing Systems may be recovered in case of any errors. The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Backup processes
- Remote encrypted storage
- Disaster Recovery Plan (DRP)
- Redundant, distributed, fail-safe storage subsystems

13. Reliability:

The Data Processor shall ensure that all functions of the Data Processing System are available and to receive notifications of all emerging system failures (reliability).

14. Data integrity:

The Data Processor shall ensure that the stored Personal Data cannot be damaged due to the failure or defective operation of the system (data integrity).

- Monitoring system with alerting in case of possible data loss

15. Monitoring of availability:

The Data Processor shall ensure that there exists an appropriate protection against accidental loss or destruction of Personal Data and thus that the Personal Data are at all times available to the Data Processor (monitoring of availability). The Data Processor therefore applies at least the following measures (please indicate the relevant):

- Saving processes/back-up copies
- Mirroring hard-drives, e.g. RAID technology
- Distributed, fail-safe storage systems
- Certified datacenters (SOC-1 Type II, PCI-DSS, ISO 27001, TVRA, ISO 9001, Type II SOC-2 – whereas applicable)
- Disaster Recovery Plan (DRP)
- Geo-redundancy (upon request)

16. Pseudonymisation of Personal Data:

The Data Processor shall ensure the appropriate pseudonymisation of Personal Data upon request.

17. Regular testing procedures regarding the measurement and assessment of technical and organizational measures:

The Data Processor shall ensure the regular testing, measuring and assessing of the effectiveness of the technical and organizational measures applied in order to guarantee the security of Personal Data. The Data Processor therefore applies at least the following measures (please indicate the relevant).

- Data Protection Management, DPM
- Incident Response Management
- Regular stress-tests