Attachment 1
Technical-organizational measures according to §32 GDPR, status 28.06.2018

Tandberg Data GmbH
Feldstraße 81
44141 Dortmund
Germany

Tel: +49 (0)231 5436 – 0
Fax: +49 (0)231 5436 – 111

tandbergdata.com

Question 1: Topic: I. Confidentiality (§ 32 (1) (b) GDPR)
Access control / What measures have been taken to prevent unauthorized persons from gaining access to data processing systems?

1. Alarm systems
2. Electronic access control system
3. Photoelectric sensors / motion
4. Key regulation (key output etc.)
5. Video surveillance of entrances
6. Video surveillance of outside

Question 2: Topic: I. Confidentiality (§ 32 (1) (b) GDPR
Access control / What measures have been taken to prevent the use of data processing systems by unauthorized persons?

1. Assignment of user rights
2. Requirements for Secure Passwords (described in Business Process Narrative - Security and Access Controls - IT Controls 1-2-3.docx)
3. Authentication with username / password
4. Secure passwords for smartphones
5. Use of individual user names
6. Using VPN technology (remote access)
7. Encryption of mobile data carriers

Question 3: Topic: I. Confidentiality (Section 32 (1) (b) GDPR)
Access Control / What measures have been taken to prevent unauthorized reading, copying, alteration, removal within the data processing systems?

1. Authorization concept
2. The number of administrators has been reduced to the "necessary"
3. Log access to applications, especially when entering, changing and deleting data
4. Physical deletion of media before reuse
5. Secure storage of data media
6. Use of anti-virus software

7. Use of a software firewall
8. Administration of rights by system administrator
9. Use of a hardware firewall
10. Password policy incl. Password length, password change (limited validity)
11. Proper destruction of paper (use of shredders or service providers)

Question 4: Topic: I. Confidentiality (§ 32 para 1 lit. b GDPR)
Separation control / What measures have been taken to ensure that data collected for different purposes are processed separately?

1. Separation of productive and test systems

Question 5: Topic: I. Confidentiality (§ 32 para 1 lit. b GDPR)
Pseudo anonymization / What measures have been taken to ensure that personal data is processed in such a way that it can no longer be assigned to a specific data subject without the need for additional information?

1. None of the above measures have been taken

Question 6: Topic: II. Integrity (§ 32 para. 1 lit. b GDPR)
Follow-up control / What measures have been taken to prevent personal data from being read, copied, altered or removed during processing, electronic transmission or transport by unauthorized persons?

1. Establishment of leased lines or VPN tunnels
2. Encrypted data transmission (e.g., https or SFTP)

Question 7: Topic: II. Integrity (Section 32 (1) (b) GDPR)
Input control / What measures have been taken to determine if and by whom personal data has been entered, altered or removed from computer systems?

1. Dedicated assignment of rights for entering, changing and deleting data based on an authorization concept
2. Logging of input, modification and deletion of data
3. Traceability of input, modification and deletion of data by individual user names (not user groups)

Question 8: Topic: III. Availability and resilience (§ 32 (1) (b) GDPR)
Availability Control / What measures have been taken to protect personal information when processing accidental destruction or loss?

1. Uninterruptible power supply (UPS)
2. Devices for monitoring temperature and humidity in server rooms
3. Retain the backup in a secure, outsourced location
4. Regular check of system states
5. Regular backup of databases
6. Backup and Recovery Concept (described in Business Process Narrative - Business Continuity - IT Controls 5-6-7.docx)

7. Regular backup of files
8. Air conditioning in server rooms
9. Emergency Plan (described in Business Continuity Plan v1.docx and Disaster Recovery Plan v1.docx)

Question 9: Topic: III. Availability and resilience (§ 32 (1) (b) GDPR)
Recoverability / What measures have been taken to ensure that the systems that process personal data are able to recover quickly after an incident?

1. Recovery concept
2. Testing Data Recovery

Question 10: Topic: IV. Procedures for regular review, validation and evaluation (§ 32 (1) (b) GDPR)
Data protection management / Which measures, and processes have been implemented in-house regarding the organization of data protection?

1. A data protection officer is named in writing
2. The DPO is involved in the data protection follow-up assessment
3. Employees have been committed to data secrecy / the handling of personal data
4. There is a list of processing activities (LPA)

Question 11: Topic: IV. Procedures for regular review, validation and evaluation (§ 32 (1) (b) GDPR)
Incident management / What measures have been implemented regarding the response to detected or suspected security incidents or disruptions in IT areas?

1. No incident management was implemented due to the size of the company

Question 12: Topic: IV. Procedures for regular review, validation and evaluation (§ 32 (1) (b) GDPR)
Data protection through technology design and privacy-friendly preferences / Which measures, and processes have been implemented in order to ensure up-to-date data protection both in advance and during ongoing processing?

1. Work instruction to observe "privacy be default"

Question 13: Topic: IV. Procedures for regular review, validation and evaluation (§ 32 (1) (b) GDPR)
Order control / What measures have been taken to ensure orderly and order-based order processing across the entire processing chain?

1. It is ensured that the employees of the processor are committed to data secrecy / confidentiality
2. It shall be ensured that the processor has appointed a data protection officer if required by law