Willing & Able
Technical and Organizational Measures

1. Access Control

a) Alarm system.
b) Manual locking system.
c) Video surveillance.
d) Visitors: Only accompanied by employees.
e) Security locks.

2. Data Carrier Control

a) Encryption of data carriers.
b) Use of document shredders.
c) Secure erasure of data.

3. Memory Control

a) Encryption of data carriers.
b) Use of document shredders.
c) Secure erasure of data.

4. User Control

a) Encryption of data carriers.
b) Use of anti-virus software.
c) Defining database rights.
d) Creating of user profiles.
e) Automatic desktop lock.
f) Authentication with username / password.
g) Withdrawal of access rights when people are leaving the company.

5. Access Authorization Control

a) Use of anti-virus software.
b) Careful selection and verification of service providers and processors.
c) Limitation of the number of administrators.
d) Withdrawal of access rights when people are leaving the company.
e) Secure erasure of data carriers.

f) Encryption of mobile IT systems.

g) Encryption of mobile data carriers.

h) Two-Factor-Authentication.

6. Transmission Control

a) Logging of access.

b) Use of signature procedures.

c) Use of encryption technologies.

7. Data Entry Control

a) Assignment of rights for the entry, modification and erasure of data.

b) Storage of logs of entries, changes and erasure.

8. Transport Control

a) Encryption of email.

b) Safe transport containers.

c) Careful selection of the transport staff and vehicles.

9. Recoverability

a) Test of data recovery.

b) Storage of data backup in a safe and outsourced place.

c) Regularly backups.

10. Reliability

a) Keep redundant systems available for emergencies.

b) Anti-virus protection.

11. Data Integrity

a) Regular backups of the whole system.

b) Storage on several and different devices.

12. Processor Control

a) Selection of each processor in the light of care aspects.

b) Documentation of the TOMs taken by processors.

c) Effective control rights are agreed with each processor.

d) Written agreements with processors (contracts).

13. Availability Control

a) Secure and Trustful Hosting Providers.

b) Storage of data backup in a safe and outsourced place.

c) Test of data recovery.

14. Separation Control

a) Defining database rights.

b) Definition of data records with purposeful attributes / data fields.

c) Separation between the productive system and test systems.

15. Pseudonymisation

a) Pseudonymisation of Personal Data no longer needed in plain text.

b) Pseudonymisation of data in test systems.

16. Encryption

a) Encryption of data carriers.

b) Encryption of websites (SSL).

c) Encryption of passwords in databases.

17. Resilience

a) Use of an uninterruptible power supply (UPS).

b) Use of load balancing.

18. Process for regularly testing, assessing and evaluating the effectiveness of Technical and Organizational Measures

a) Regular TOM audits.

b) Regular training of employees.

c) Regular review of processing activity records.

d) Review of privacy by design.

e) Ensuring privacy by default settings.

f) Implementation of a process for Data Protection impact assessments.

g) Implementation of a Data Protection handbook.

19. The procedure for regular examination, assessment and evaluation of the effectiveness of the Technical and Organizational Measures to ensure a Data Protection compliant processing

Audit of the TOMs by external Service Provider.