Description of the technical and organisational measures

1. General organisational measures

Measures suitable for creating awareness for data protection. The following general organisational measures have been implemented by the contractor:

- A data protection officer has been appointed
- Employees receive data protection training courses/instructions (type of training: face-to-face training)
- Data protection training courses are repeated
- Employees have been/will be obligated to keep operational/trade secrets
- Employees have been/are obligated to data secrecy
- Employees sign confidentiality agreements

2. Pseudonymisation/Encryption

(Art. 32 para. 1 lit. a EU GDPR)

Measures to ensure the protection of personal data by converting the data into a pseudonymised form using auxiliary mechanisms and processing them, or by protecting them against access through state-of-the-art encryption:

- Storage takes place on encrypted data carriers and secured servers.
- Use of sound, state-of-the-art encryption (Bitlocker, FileVault).
- Encrypted storage of personal data on mobile data carriers (notebook, smartphone, USB stick, etc.).

- Mobile devices (especially laptops) have hard disc encryption by default.
- Data are encrypted and then transmitted to other areas or processors in an encrypted form.
- Backups of the database are AES-256 encrypted before long-term storage.

3. Confidentiality

(Art. 32 para. 1 lit. b EU GDPR)

Measures to ensure the confidentiality of the systems and services when processing personal data.

- **Appropriate access controls to the premises, buildings, and server rooms:**
  - Area cannot be left unnoticed through several doors (emergency exits)
  - Careful selection of cleaning staff
  - Locking system to access the company premises/office spaces with:
    - Keys
    - Key issuance is logged
  - Visitor regulations in place
    - Visitors are always accompanied on the premises
- **Appropriate data carrier checks:**
  - Keeping an inventory list of all data carriers in the infrastructure
  - Regular checks of whether the storage of personal data is necessary (scope and purpose)
  - Proper destruction/deletion of data/data carriers/paper:
    - Physical deletion of data carriers so as not to be reused
    - Proper destruction of paper (DIN 66399):

    Security level P-4
- **Appropriate user management, as well as dedicated user and authorisation concept:**
  - Unique user identification
  - Central creation of users
  - Application based on the four-eyes principle
  - Allocation of user rights
  - Creation of user profiles
  - Initial password with obligation to change
  - Training on passwords

- Authentication with username/password
    - Allocation of user profiles to IT systems
    - Management of rights by the system administrator
    - Number of administrators reduced to the “bare minimum”
- **Appropriate user control measures:**
    - Only authorised persons and devices are granted access
    - Users must authenticate themselves for network logins
    - There is a secure WLAN (at least WPA2):
    - Use of a software firewall
    - Regular checks of the firewall settings
    - Remote maintenance access is only permitted when required
    - User accounts of employees who have resigned will be blocked immediately
    - Use of private mobile devices (among others, laptops, tablet PCs, smartphones), e.g. allowed within the framework of a bring-your-own-device rule

- **Protection when transmitting personal data:**
    - Type of protection of the data between the customer and contractor: encryption
- **Measures for order control**
    - Selection of subcontractors with diligence considerations (especially in regard to data protection)
        - Based on the agreement for data processing on behalf
        - Based on further documents: Standard contractual clauses, Privacy Shield certification
        - Documentation on suitability can be accessed
    - Agreements with the service providers include:
        - There is an agreement according to Art. 28 for each service provider
        - Further sub-service providers are subject to approval
        - The contractor has appointed a data protection officer

Service providers are commissioned for:

- Telephone system
- Payroll

- **Further measures for purpose limitation/the separation rule**
    - Specification of database rights

4. Integrity

(Art. 32 para. 1 lit. b EU GDPR)

Measures to ensure the integrity of the personal data processed.

- Remote maintenance access is only permitted when required
- Selection of subcontractors with diligence considerations (especially in regard to data protection)
- **Measure for separability**
    - Separation of the productive and test systems
    - Specification of database rights

5. Availability

(Art. 32 para. 1 lit. b EU GDPR)

Measures and guarantees that personal data are protected against destruction or loss.

- **Measures to ensure availability**
    - Creation of a backup & recovery concept
    - Scope of protection:
        - Databases
        - File servers
    - Type of protection:
        - Band
        - Hard drive
        - On another system
- **Measures for recovery**
    - Contingency plans in place/up to date
    - Testing data recovery, frequency: annually

- **Measures for availability checks**
    - Uninterruptable power supply (UPS) is installed
    - Air conditioning in the server rooms
    - Devices to monitor temperature and humidity in the server rooms
    - Storage of data backups:
        - in a secure, outsourced location (type of data transmission: digital, encrypted)

- Use of cloud services
  - Amazon Cloud
  - Google Docs

6. Resilience of the systems

(Art. 32 para. 1 lit. b EU GDPR)

Guarantee that IT systems will function properly even under high usage frequency (performance). The dependability of the IT systems is essential for maintaining business operations, i.e. for business continuity. The term "resilience" refers to the dependability or capacity of the systems or services.
Measures to ensure the resilience of systems and services:

- **Measures for resilience**
  - Redundant WAN connections
  - Multi-channel bonding (e.g. UMTS/LTE/glass fibre/copper)
  - Sufficient dimensioning of the storage systems
  - Sufficient dimensioning of the working memory
  - Monitoring the systems
  - Monitoring the network
  - Failure rate statistics
  - Availability statistics
  - Ticket system
  - Service Level Agreements (SLA) concluded with service providers
  - Uninterruptible power supply (UPS) is installed
  - Air conditioning in server rooms
  - Devices to monitor temperature and humidity in server rooms
  - Adequate dimensioning of storage systems
  - Adequate dimensioning of working memory

7. Long-term processing

(Art. 32 para. 1 lit. b EU GDPR)

Measures to ensure that processing is guaranteed in the long term with integrity and, on the other hand, that the duration of processing is not exceeded.

- Monitoring the systems
- Monitoring the network
- Data backup formats enable long-term backup and recovery
- Change management available; updates are only done, for example, after prior tests

8. Recovery

(Art. 32 para. 1 lit. c EU GDPR)

Measures to ensure that systems and services for processing personal data can be recovered in the event of a fault.

- Backup procedures available according to categorisation and resources
- Accessibility of administrators regulated (on-call service, if necessary)
- Existence of backup data centres (hot site, warm site, cold site)
- Service Level Agreements (SLAs) concluded with service providers

9. Storage restriction

(Art. 5 para. 1 lit. e EU GDPR)

Ensuring that personal data are stored in a form that only allows the identification of the data subjects for as long as is necessary for the purposes for which they are being processed; personal data may be stored for longer if the personal data, subject to the implementation of suitable technical and organisational measures required by this regulation to protect the rights and freedoms of the data subject, are exclusively processed for archiving purposes in the public interest, or for scientific and historical research purposes, or for statistical purposes in accordance with Article 89 paragraph 1 (“storage restriction”).

The following measures for storage restriction are implemented by the contractor:

- Existence of a deletion concept (especially for CRM and ERP systems)
- Evidence of data deletion through system logs

10. Regular evaluation of effectiveness

(Art. 32 para. 1 lit. d EU GDPR)

A procedure for the regular review, assessment, and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing.
The following measures for the regular evaluation of effectiveness are implemented by the contractor:

- Evaluation of incidents
- Evaluation and implementation of suggestions for improvement
- Review of the management systems by the management
- Review by the DPO (with report)