Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the Contractor shall, in its capacity as data processor, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, but not limited to, the following:

1. Pseudonymization

Pseudonymization means the processing of personal data of the Customer in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separate and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

2. Confidentiality

2.1 Physical access control

The Contractor shall take appropriate measures to reduce the risk of unauthorized persons gaining access to data processing systems with which the Customer's personal data are processed and used. Measures to control access may include, for example, automatic access control systems, use of chip cards and transponders, control of access by gatekeeper services and alarm systems. Servers, telecommunications systems, network technology and similar equipment can be protected, for example, by lockable server cabinets. It also makes sense to control access by means of organizational measures (e.g., service directives stipulating that service rooms are to be locked when employees are absent).

Technical measures:

- Automatic access control system
- Chip cards / transponder systems
- Manual locking system
- Doors with outside knobs

Organizational measures:

- Key regulation (key surrender, etc.)
- Visitors accompanied by employees
- Careful selection of cleaning personnel

2.2 System access control

The Contractor shall take appropriate measures to prevent data processing systems (computers) from being used by unauthorized persons.

For this purpose, the Contractor shall take the following precautions:

Technical measures:

- Login with username + password
- Partial login with biometric data
- Smartphone encryption
- Encryption of laptops / tablets
- Laptop management
- Use of anti-virus software for servers
- Deployment of anti-virus software for clients
- Automatic desktop lock

Organizational measures:

- Manage user permissions
- Create user profiles
- Bring-Your-Own-Device policy
- Mobile Device Policy
- General policy on data protection and / or security

2.3 Data access control

The Contractor shall take appropriate measures to ensure that the persons authorized to use the data processing systems can only access the personal data subject to their access authorization and that personal data of the Customer cannot be read, copied, modified or removed without authorization during processing, use and after storage. For this purpose, the Contractor shall take the following precautions:

Technical measures:

- Physical erasure of data carriers on laptops before reuse.
- Logging of access to important documents, especially when entering, changing and deleting data.
- File shredder (min. level 3, cross cut)

Organizational measures:

- Creating an authorization concept
- Management of rights by system administrator

- Reduction in the number of administrators
- Closed area for sensitive documents

2.4 Separation control

The Contractor shall take appropriate measures to ensure that personal data of the customer collected for different purposes can be processed separately. For this purpose, the Contractor shall take the following precautions:

Technical measures:

- Separate storage on segregated systems or data carriers.
- Software-based customer separation

Organizational measures:

- Creation of an authorization concept
- Determination of database rights

3. Integrity

3.1 Transmission control

The Contractor shall take reasonable measures to reduce the risk that personal data of the Customer can be read, copied, modified or removed without authorization during electronic transmission or during their transport or storage on data carriers. To this end, the Contractor shall take the following precautions:

Technical measures:

- Email encryption
- Logging of accesses and retrievals of important documents and data
- Provision *via* encrypted connections such as sftp, https
- Use of signature procedures

Organizational measures:

- Possibility of creating an overview of regular retrieval and transmission operations.

3.2 Data input control

The Contractor shall take appropriate measures to ensure that it is possible to check and determine retrospectively whether and by whom personal data of the customer have been entered into data processing systems, changed or removed. For this purpose, the Contractor shall take the following precautions:

Technical measures:

- Possibility of technical logging of the entry, modification and deletion of personal data.

Organizational measures:

● Traceability of entry, modification, and deletion of personal data through individual user names.

● Retention of forms from which personal data have been transferred to automated processing operations.

● Assignment of rights to enter, change, and delete personal data on the basis of an authorization concept.

4. Availability and resilience

4.1 Availability control

The Contractor shall take reasonable measures to ensure that personal data of the customer is protected against accidental destruction or loss. For this purpose, the Contractor shall take the following precautions:

Technical measures:

● Fire and smoke detection systems

● Careful selection of the hosting service provider

Organizational measures:

● Regular control of the hosting service provider

5. Procedures for regular review, assessment and evaluation.

The Contractor shall implement procedures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

5.1 Data protection management

Technical measures:

● Central documentation of all procedures, regulations and guidelines on data protection with access for employees as required / authorized

● A review of the effectiveness of the technical protective measures is carried out regularly

Organizational measures:

● Employees trained and committed to confidentiality

● Raising employee awareness through training

The company complies with the information obligations pursuant to Art. 13 and 14 of the GDPR. Formalized process for handling requests for information from data subjects is in place.

5.2 Incident response management

Security breach response support.

Technical measures:

- Use of spam filters and regular updating
- Use of virus scanner and regular updating

Organizational measures:

- Documentation of security incidents and data breaches
- Regulation of responsibilities for the follow-up of security incidents and data breaches

5.3 Privacy-friendly default settings (Art. 25 (2) GDPR); Privacy by design / Privacy by default

Technical measures:

- No more personal data is collected than is necessary for the respective purpose.