Annex 2 - Technical and organisational measures (according to art. 32 GDPR and § 64 BDSG).

1. Confidentiality (art. 32 (1) lit. b) GDPR)

1.1. Admission control

Measures suitable for preventing unauthorized persons from gaining admission to buildings and rooms housing data processing equipment with which personal data are processed or used

Technical measures
- Building access only with chip key
- Office access only with chip key
- Central locking system with safety locks
- Alarm system with motion sensors

Organisational measures
- Regulation of access to keys
- Named list of persons entitled to enter
- Visitors always accompanied by staff
- Careful selection of cleaning services

1.2. Access

Measures suitable for preventing data processing systems from being used by unauthorised persons

Technical measures
- Management of user profiles and permissions
- Authentication with username and password
- Use of password policies
- No local on-premise software systems
- No local servers, infrastructure exclusively in cloud data centers
- Access to databases only with SSL encryption
- Access to databases and infrastructure with 2-factor-Authentication
- Unused equipment automatically locks into password-protected mode after 5 minutes

Organisational measures
- IT policy incl. guide to manual desktop lock
- Deactivation of the permissions of leaving/ retired employees as part of an "outgoing employee" checklist

1.3. Access

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, changed or removed without authorisation during processing, use and after storage.

Technical measures
- Only digital processing of customer-related data (no printouts)
- Physical deletion of disks
- Logging of access to infrastructure and databases
- Audit logs of accesses to your own applications

Organisational measures
- Use of authorization concepts - differentiated by data, applications and operating system
- Minimum number of administrators
- Management of user rights by administrators only
- Password policy incl. password length and, if applicable, cyclic password change

1.4. Separation control

Measures to ensure that data collected for different purposes are processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical measures
- Multi-tenancy of relevant applications
- Separation of productive and test environment
- Physical separation (systems and databases)

Organisational measures
- Control via authorization concept
- Defining database rights
- Records are equipped with purpose attributes

2. Integrity (art. 32 (1) lit. b) GDPR)

2.1. Transfer control

Measures to ensure that personal data cannot be read, copied, changed or removed without authorisation during electronic transmission or during their transport or storage on data carriers and that it is possible to check to whom personal data are to be transmitted by data transmission equipment.

Technical measures
- Logging of accesses and retrievals
- Encrypted Transmission (SSL/TLS)

Organisational measures
- IT user guideline

2.2. Input control

Measures to ensure that it is possible to verify "post mortem" whether and by whom personal data have been entered, modified or removed in data processing systems. Input control is achieved through logging, which can take place at various levels (e.g. operating system, network, firewall, database, application).

Technical measures
- Technical logging of input, modification and deletion of data by audit logs
- Manual or automated control of logs

Organisational measures
- Traceability of input, modification and deletion of data by individual usernames (not user groups)
- User rights management to enter, modify and delete data (authorisation concept)
- Clear responsibilities for deleting data

3. Availability and resilience (art. 32 (1) lit. b) GDPR)

3.1. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss

Technical measures
- Use of certified subcontractors to guarantee high availability of data and services

Organisational measures
- Daily several automated backups incl. recovery opportunities
- Control of the backup process
- Regularly tests to restore data including logging of results

4. Data protection management (art. 32 (1) lit. d) GDPR; art. 25 (1) GDPR, art. 28 GDPR)

4.1. Privacy Management

Technical measures
- Central storage of all internal data protection procedures and -regulations gaining simple access for employees (e.g. wiki, intranet ...)
- A review of the effectiveness of the technical protection measures is carried out at least once a year

Organisational measures
- Employees trained on data protection and data security and committed to confidentiality/ data secrecy via a data protection obligation
- Regularly employees awareness training – at least annually
- The organisation works in compliance with the information requirements stated in articles 13 and 14 GDPR
- Formalised process for handling of "requests for information" from data subjects is available

4.2. Incident response management

Technical measures

- Use of spam filters and regular updates via e-mail providers

Organisational measures

- Documented process for reporting security incidents and data breaches
- Documentation of security incidents and data breaches
- Formal process and responsibilities for post-processing of security incidents and data breaches

4.3. Data protection by design and by default (art. 25 GDPR)

- Orientation to the basic data protection principles "privacy by design" and "privacy by default"
- No more personal data is collected than is necessary for the specific purpose
- Data queries and input forms are designed with “data protection friendly” base settings

4.4. Order control / processing on behalf of the order (art. 28 GDPR)

In the case of the processing of personal data on behalf: measures to ensure that personal data processed on behalf of the order can only be processed in accordance with the instructions of the client.

- Selection of the contractor is based on a due diligence (especially with regard to data protection and data security)
- Prior verification of the security measures taken by the contractor and their documentation
- Conclusion of a “DPA” (data processing amendment) in accordance with art. 28 GDPR or a comparable contract based on the EU commissions’ standard contractual clauses in case of processors located outside the EU/ EEA
- Written instructions to the contractor
- Obligation of the contractor's employees to keep data secret
- Appointment of a data protection officer by the contractor, if necessary
- Agreement of effective control rights against the contractor
- Regulations on the use of additional subcontractors