Technical and organizational data-protection measures

A. Organization

Technical and organizational data-protection measures meet the requirements pursuant to § 9 sentence 1 of the German Federal Data Protection Act.
The internal organization of Infopark AG and a third party mandated by it is through measures designed in such a way that it will meet the special requirements of data protection. Such measures include:
• Written procedures, guidelines, leaflets;
• Programs / procedures are properly documented;
• Storage of automated protocols / logs is regulated;
• Program approval process is established;
• Notifications, requests for information, concerns regarding rectification, erasure or blocking

B. Security measures

The servers for the online system, databases, and data protection (backup) are run and maintained at Infopark AG or mandated third parties in professional data centers. The subcontractors are selected carefully and with respect to their security awareness and their expertise checked.
Some of the relevant safeguards of the following checklist are not shown separately because it is the responsibility of subcontractors or are not published in detail for the sake of maintaining the security of confidentiality.

1. Access control

The access control to server rooms occurs by the spatial structure of the data center and there through the operator ensured control system.
During times of business operations is the entrance to the premises of Infopark AG Berlin secured by a personalized electronic key (transponder). Outside of the times of business operation, the rooms are permanently and automatically monitored by external services (security service) - closing the doors and motion detection. In addition, the outer doors of the building outside of times of the business are closed mechanically. An access control by staff in the reception area occurs during times of the business operations. The entrance area and the technology sector are secured with optical space surveillance (video).
2. Admission control

2.1. The unauthorized use of computer systems is prevented by:
   • Password assignment and
   • Recording of incorrect password attempts.

2.2. Each owner has his own password known only to him, which may not be distributed. In case of any disclosure of the password, this has to be changed immediately.

2.3. For all activities related to the DP system, reports shall be created automatically.

2.4. The protocols shall be evaluated by the system administrator on a regular basis as well as in case of deviations (for example, very high activity).

2.5. The data transfer to and from the computer system will be secured in critical activities (for example, system maintenance, software updates, and backups) against unauthorized use through the following measures:
   • Automatic callback from the server to the user’s known IP;
   • Review of known public key known when contacting;
   • Encrypted data transmission (SSL / SSH);
   • Logging of system usage and protocol analysis.

3. Access control

3.1. The unauthorized reading, copying, modification or deletion of data is prevented by:
   • Appointment of the person responsible for the media;
   • Software-based exclusion (authorization concept);
   • Software-based monitoring of implausible use (monitoring);
   • Secure interfaces;
   • Further control mechanisms of the data center.

3.2. The media are kept on the DV equipment outside of working time. Pure Backup media are located in a locked cupboard (storage in the data according to exacting rules).

3.3. Only relevant data media are kept for the particular workspaces. Developers have access only to fictitious test data. By interferences, authorized personnel can access real data to the extent necessary to eliminate interference.

3.4. The Disk Management is performed by a given scheme (Instructions).
3.5. The restriction of access possibility of beneficiary for using a data processing system exclusively on the data authorized for his access authorized, is guaranteed through:

- Automatic check of access authorization using a password;
- Exclusive menu control depending on the authorization;
- Differentiated access rights to applications;
- Sophisticated editing capabilities (read / change / delete).

4. Transfer control

4.1. A physical dispatch of data medium is not foreseen.

4.2. Private media should not be used in the data center (regulation by the data center).

4.3. Magnetic disks that are no longer used shall be destroyed by multiple overwriting (regulation by the data center).

4.4. The unauthorized reading, copying, modification or removal of data during transfer is prevented by:

- SSL and SSH encryption of data transmission;
- Completeness checks if relevant;
- Development of the transport connection only between defined and secured certificates of systems.

4.5. The transport process automatically confirms the receipt of the software data.

4.6. All sensitive data provided for transport are encrypted.

4.7. The transfer of personal data occurs by use of the following services:

- Regular WWW (HTTPS);
- Other services and transport methods that require equivalent or better state of security

The following security measures are in:

- Hardware and software firewall;
- Intrusion Detection System;
- Programs to prevent the penetration of viruses and detect the intrusion.

4.8. At what points the data transmission is provided through data communication equipment, can be taken from the documentation of the transfer points and transfer channels.
5. **Input control**

5.1. Whether and by whom the data can be entered in computer systems, modified or removed, can be later checked and determined through:
   • User identification;
   • Logging of input data (application protocol).

6. **Order control**

6.1. There are contracts for the following types of order processing:
   • Maintenance / remote maintenance;
   • Administration / remote administration.

6.2. The processing of personal data on behalf of orders given by the Contactor shall be ensured only by written agreement between the Contactor and the Customer or the data center.

6.3. If serious changes occur in the process, the Customer shall be informed through the Contactor.

6.4. The Customer shall be informed about program crashes and bugs.

6.5. The security of remote maintenance is not applicable as there is no remote control by the Customer.

7. **Availability Control**

7.1. The data security from accidental loss or destruction is guaranteed by:
   • Use of RAID disk systems;
   • Software exclusion: Breakdown of the servers for independent and autonomous fulfillment of the tasks (shared nothing architecture);
   • Multiple incremental database and database system backups;
   • Backups with a timetable which appropriately reflects data changes while using;
   • Multiple, separate storage of backup data;
   • Additional manual backup option of the Customer;
   • Additional measures of the data center.

7.2. A plan for a disaster situation is available.

7.3. The system can be operated at geographically separated data centers (alternate data center).
8. Separation rule according to the principle of earmarking

8.1. Personal data are permitted to be used only for the purpose for which they were originally collected.

8.2. That the data collected for different purposes can be processed separately, is guaranteed by:
   • Software exclusion (client separation; multi-tenant architecture);
   • The database principle, separation by access control;
   • Separation of test and production data;
   • Separation of development and production programs.