**Fundamental requirements for information security**

**For contracts with IT-supported processing of data from cellcentric.**

1. The contractor undertakes to always effectively secure all information and data that the contractor collects or processes for the client, or to which it has access, against unauthorized access, modification, destruction or loss, unauthorized transmission, other unauthorized processing and other misuse in accordance with the current state of the art. The contractor has a suitable security concept for this purpose.

2. The contractor shall coordinate its security concept with the client. In particular, the stipulations and specifications for information security defined in the requirements or in other written requirements must be complied with and taken into account for the security concept. The responsible information security officer of the client provides support. The client may demand suitable, regularly written proof of the implementation of and compliance with the security concept. In case of any doubts, the contractor shall also enable the client to visit the site and provide necessary information.

3. The contractor shall appoint a contact person for security management with sufficient authority who is available for all information security topics, e.g. for incident management (management of information security incidents).

4. The contractor shall inform the client in text form of any significant changes to the data processing. Changes are particularly significant if they affect the security concept. The notification must describe the scope of the change and the impact on the security concept. In the event of a foreseeable reduction in the protective effect, the client's consent must be obtained in text form before the change is made.

5. The client's information and data may only be used by the contractor for the contractually agreed purposes and to the extent necessary for the performance of the contract. When processing data from different clients, data separation must be ensured and subject to verification (client separation).

6. Access to data processing systems ("DP systems") of the client or its subcontractors may only take place with the permission of the client to the extent permitted and necessary for the performance of the contract by the persons authorized to do so. The contractor undertakes not to disclose to any unauthorized person the access authorizations assigned to it for the use of the system. The contractor shall only be permitted to allow any subcontractors or freelancers to access the data processing systems of the client, its agents or subcontractors to the extent required by the contract with the client's consent. The contractor must notify the client without delay if employees of the contractor, subcontractors or freelancers with access or access authorizations for data processing systems of the client, its agents or subcontractors are no longer involved in the performance of the contractual service, so that the client can revoke existing access and access authorizations.

7. All information of the client classified as confidential or secret shall be protected by the contractor by suitable cryptographic measures according to the latest technological standards during transmission, as well as during storage on mobile data carriers; this shall not be required in the case of transmission or storage within a secured environment. Upon request of the client, the contractor shall prove that the environments are designed for the processing of confidential or secret data in accordance with the latest technological standards.

8. The contractor shall immediately inform the client in case of becoming aware (or in the event of a justified suspicion) of data protection violations, security breaches and other manipulations of the processing sequence affecting cellcentric data and services, and shall immediately – in coordination with the client – take all necessary steps to clarify the facts and to limit the damage.

9. If the data processing takes place at cellcentric or in data exchange with cellcentric systems, the contractor shall, if necessary, take appropriate measures to ensure that there is no interference with the cellcentric infrastructure (and third parties from within the cellcentric environment). The contractor shall comply with the client's applicable information security requirements.

10. The contractor shall inform the client immediately if there is a risk that unauthorized persons access data of cellcentric due to seizure, confiscation or other official access, in insolvency or composition proceedings or due to other events or measures of third parties. The contractor will inform the third parties that the data is from cellcentric.

11. The contractor shall regularly inform its employees, subcontractors or freelancers with access authorizations for the client's data processing systems about relevant information security topics in connection with the provision of services vis-a-vis the client.