1. **Technical and organisational measures of the archive holder**

Documentation of the technical and organisational measures to be taken in accordance with 32 GDPR[[1]](#footnote-1) .

|  |  |  |
| --- | --- | --- |
| 1. | **Pseudonymisation**  How is the pseudonymisation of the data guaranteed?  Pseudonymisation is the processing of personal data in such a manner 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 separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person. | Personal data is processed by  Random codes replaced  Data Masking  Other: |
| 2. | **Encryption**  How is encryption guaranteed?  Encryption transforms plain text into an associated ciphertext (ciphertext) depending on additional information called a "key", which should be indecipherable for those who do not know the key. | Use of cryptographic tools  Data hashing  Encryption of storage media  Encryption of communication  Other: |
| 3. | **Ability to maintain confidentiality**  How is data confidentiality guaranteed in the long term?  Confidentiality means that personal data is protected against unauthorised disclosure. | Electronic access control system  Security doors and/or windows  Grilles in front of windows and doors  Plant security, gatekeeper  Alarm system  Video surveillance  Special protective measures for the server room  Customised log-in and password procedure  Additional log-in for certain applications  Automatic blocking of clients (timeout)  Management of authorisations  Documentation of authorisations  Encryption of systems  Encryption of communication  Encryption of data carriers  VPN (Virtual Private Network)  Secure WLAN  SSL encryption for web access |
| 4. | **Ability of integrity**  How is the ability to ensure the integrity of the data permanently guaranteed?  Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is applied to "data", it means that the data is complete and unchanged. | Measures should be taken to prevent damage/alteration of the protected data during processing or transmission  Use of access rights  System logging  Functional responsibilities  Other: |
| 5. | **Availability capability**  How is the ability to make data available permanently guaranteed?  The availability of services, functions of an IT system, IT applications or IT networks or even information is ensured if these can always be used by users as intended. | Back-up procedure  Mirroring hard disks  Uninterruptible power supply (UPS)  Virus protection /Firewall  Emergency plan  Air conditioning systems  Fire and extinguishing water protection  Alarm system  Suitable archiving facilities  Other: |
| 6. | **Ability to work under pressure**  How is the resilience of the data guaranteed in the long term?  Systems are resilient if they are so robust that they can function even under heavy access or heavy utilisation. | Penetration tests  Other: |
| 7. | **Recoverability of availability and access**  How is it ensured that personal data is quickly available and accessible again after security incidents? | Back-up procedure  Uninterruptible power supply (UPS)  Emergency plan  Substitution rules  Other: |
| 8. | **Procedure for regular review\***  How is it ensured that the aforementioned data backup measures are regularly reviewed? | There is a defined test routine  Test reports are evaluated  Implementation of suggestions for improvement |
| 9. | **Unlawful access to personal data**  How can data processing systems be prevented from being used by unauthorised persons? | Customised log-in and password procedure  Additional log-in for certain applications  Automatic blocking of clients (timeout)  Management of authorisations  Documentation of authorisations  Encryption of systems  Other: |
| 10. | **Processing of personal data only according to instructions**  How is it ensured that personal data is only processed in accordance with the controller's instructions? | Employees are obliged to observe rules of conduct  Implementation of internal company data protection guidelines  Obligation of employees to maintain data secrecy  Training for all authorised employees  Determination of contact persons and responsible project managers for the specific order |

1. This document serves to fulfil legal requirements and is intended to provide a **general** description that enables a **preliminary assessment to be made of** whether the data security measures taken are appropriate for the aspects addressed below. During the term of the contractual relationship, this data security concept must be continuously adapted and updated to reflect the current circumstances of order fulfilment. All adjustments and changes to the procedures for the fulfilment of the contract must be documented in writing. The document is part of the contract and must be submitted to the jointly responsible party in the event of significant changes and otherwise annually. [↑](#footnote-ref-1)