|  |
| --- |
| **Technical and Organizational Measures in Accordance With Art. 32 of the General Data Protection Regulation** |

**If the Contractor has a computer center, the technical and organizational measures must be stated separately for the computer center and for the Contractor's offices.**

Please state and provide proof of the **specific** technical and organizational measures you implemented to guarantee data protection and data security.

The technical and organizational measures in accordance with Art. 32 of the General Data Protection Regulation and described hereafter are not designated for the public. Only company data protection officers, competent data protection supervisory authorities and authorized employees of the respective data processing office may access to this information.

**Following a review by the Principal**,the technical and organizational measures described hereafter will be binding—as a part of this Data Protection Contract: They are specified between the Contractor and the Principal as follows:

# Abbreviations

* DC: Datacenter
* B: softgarden Office Berlin
* SB: softgarden Office Saarbrücken

# Confidentiality

## **Entrance Control**

softgarden ensures that unauthorized persons have no access to the office, server and archive rooms. This is done by:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Central reception area | X | X | - |  |
| Access through an alarm system with activated guard | X | - | - |  |
| Access with coded keys and key issue only to authorized persons | X | X | X |  |
| Logging of locks | X | X | X |  |
| Definition of the authorized persons including their documentation for employees and non-employees (maintenance staff, visitors) / gatekeepers, plant protection | X | X | - | Lead a list of visitors at the reception in Berlin |
| Foreign companies, maintenance personnel and visitors may only enter the premises accompanied by an employee | X | X | X |  |
| Legitimation of the authorized persons (key, PinCode) | X | X | X |  |
| 2-factor authentication access | X | - | - |  |
| Withdrawal of access permissions after expiry of the authorization | X | X | X |  |
| There are security areas with different access authorizations | X | X | X |  |

## **Admission Control**

softgarden prevents IT systems from being used by unauthorized persons. This is done by:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Creation of a user account per user | X | X | X | Use of non-personal support accounts for access to customer systems, access data are only accessible to authorized employees |
| Authentication of persons authorized to process data by means of a password procedure (with special characters, minimum length 8 characters, regular password change) | X | X | X |  |
| Automatic blocking of the user account in case of multiple incorrect entry of access data | X | X | X |  |
| Automatic locking of the workplace during inactivity | X | X | X |  |
| Immediate blocking of authorizations when leaving employees (directive / work instruction) | X | X | X |  |
| Regular control of the validity of permissions | X | X | X |  |
| The use of lockable cabinets for storing paper files | X | X | - | no file storage at office Saarbrücken |
| Secure transmission of authentication secrets (credentials) in the network via TLS / HTTPS, SSH, VPN (IPSec, openVPN) | X | X | X |  |
| Access IDs to workstations are manually locked during extended absence of the respective employee (30 days) and must be manually unlocked by the IT administration after return. | X | X | X |  |

## **Access Control**

The Contractor ensures that the persons authorized to use data processing systems can only access the data that is subject to their access authorization and that personal data may not be read, copied, edited or deleted without authorization during processing, use or storage.  
This is achieved through:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Definition of access authorizations for the access to data (creation of an authorization concept) | X | X | X |  |
| Defining the powers to note, input, alteration and deletion of data processed as part of the contractor's fulfillment of the contract | X | X | X |  |
| Regular control of access, input, modification and deletion | X | - | - |  |
| Disposal of unwanted data carriers (directive / work instruction) | X | X | X |  |
| Written rule for copying data (IT security guideline / work instruction) | X | X | X |  |
| Assignment of minimum authorizations (Need-to-know principle) | X | X | X |  |
| No assignment of generic or group IDs or passwords | X | - | - | Use of non-personal support accounts for access to customer systems, access data are only accessible to authorized employees |
| Avoid concentration of functions - Separate functions of administrator activities to different qualified persons | X | X | X |  |
| Maintain a history of administrative changes | X | X | X |  |
| Access to the production infrastructure via VPN | - | X | X |  |

## Separation control

softgarden ensures that data collected for different purposes can be processed separately. There is no need for a physical separation; a logical separation of the data is sufficient. This is done by:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Identification of the collected data (file number ID, customer / transaction number) | X | X | X |  |
| Logical separation of data processed for different clients Separation of functions / production / test | X | X | X |  |
| The personal data of the respective client are logically separated by assignment to the respective user account. | - | X | X |  |

# Integrity

## **Transmission control**

softgarden guarantees that personal data cannot be read, copied, edited or removed during electronic transmission, when being transported or when being saved and that where personal data transmissions via data transmission facilities are scheduled can be determined and reviewed. This is achieved through:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Determining the persons authorized to transmit or transport (electronically, manually) | X | X | X |  |
| Checking the data for completeness after data transport, transmission and data transmission or storage | X | X | X | Manual comparison with checksums |
| Implementation of security gateways at the network transfer points | X | X | X |  |
| Use of a recognized encryption method that encrypts all communications between the applicant and the contractor's servers. | X | X | X |  |
| Incoming and outgoing data streams are filtered by a modern, cascaded firewall solution | X | X | X |  |
| As far as data carriers are transmitted by transport companies, the data carriers are only forwarded after prior authentication of the transport company. | X | X | X |  |
| Paper and data media containing personal data are disposed of by a qualified disposal company in accordance with data protection laws. | X | X | X |  |
| The complete, privacy-adequate and permanent deletion of data carriers containing personal data is logged. The logs are kept audit-proof for at least 12 months. | X | X | X |  |

## **Input Control**

softgarden ensures that whether and by whom personal data is entered into, edited on or removed from data processing systems can be subsequently determined and reviewed. This is achieved through:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Management of a documentation of the access authorizations (work instruction access groups and access authorization) | X | X | X |  |
| Recording of activities under the contract | X | X | X |  |
| Random control and evaluation of the protocol data for abuse | X | - | X |  |
| For all users who use the respective application programs for the processing of personal data, a history is kept, which records which user when which action has been performed, if this action modifies personal data. | - | X | X | Capture history in the Just Hire application |

# Availability and Resilience

## **Availability Control**

softgarden ensures the protection of personal data from random or intentional destruction or loss. This is achieved through:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Uninterruptible power supply (UPS) | X | X | X |  |
| Virus protection (on workstations) | X | X | X | Virus protection on windows workstations |
| Virus protection (on servers) | X | X | X |  |
| Firewall | X | X | X |  |
| Emergency plan | X | X | X |  |
| Georedundant datacenter | X | - | - |  |
| Central fire alarm system | X | X | - |  |

## Restorability

softgarden  guarantees that the availability of and access to personal data can be rapidly restored through the following measures in case of physical or technical incidents.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Backup procedure acc. Backup concept (daily, weekly, monthly) | X | X | X |  |
| Storage of backup data in data cabinets, safes, in the other fire compartment | X | X | X |  |

# Procedures for periodic review, evaluation and evaluation

## **Dataprivacy management**

softgarden ensures a process of periodic review and evaluation of the effectiveness of technical and organizational safeguards. This is done by:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Instructing all employees about and subjecting them to data protection secrecy obligations (Art. 28(3) Letter b of the General Data Protection Regulation) | X | X | X |  |
| Regular rating of the privacy level by the privacy group | X | X | X |  |
| Third parties must submit a confidentiality statement | X | X | X |  |
| If functional overlaps exist for organizational reasons, the four-eyes principle is applied and documented. | - | X | X |  |
| Defined rules of representation within functional groups | - | X | X |  |

## **Assessment of the appropriate level of protection (Art. 32 Sec. 2 GDPR)**

softgarden guarantees a documented assessment of an appropriate level of protection, in terms of the risks associated with the processing - in particular by destruction, loss, alteration, unauthorized disclosure or access - of the personal data processed in the order. This is done by:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Carry out a risk analysis for the processing of personal data | X | X | X |  |
| Creation of protection requirement categories | X | X | X |  |
| Alignment of processes according to "Privacy by Design & Default" | - | X | X |  |
| If necessary, the implementation of a Data protection impact assessment | X | X | X |  |

## **Order Control (Art. 32 Sec. 3 and 4 GDPR)**

softgarden guarantees that personal data processed in the order will only be processed in accordance with the instructions of the client and for the fulfillment of the contractually defined purpose. The client can prove this by means of a type approval pursuant to Art. 40 or an approved certification procedure pursuant to Art. 42 GDPR. If there is no certification, proof is provided by:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **DC** | **B** | **SB** | **Remarks** |
| Clear contract design with subcontractors | X | X | X |  |
| Formalization of the order | X | X | X |  |
| Regular control of activities | X | X | X | Monitoring of softgarden processes through internal audits |
| The authorized representatives of the client and the persons authorized to receive instructions are defined by contract, and instructions are always given in written form. | X | X | X |  |
| softgarden informs the client immediately about cases of data breaches, suspected violations of data protection, if errors are detected or other irregularities in the handling the clients data. | X | X | X |  |
| Orders are recorded as a support ticket (minimum details: customer / customer, action / partial order, exact specification of the processing steps / parameters, processor, dates, recipients if necessary), where the work performed is documented. There is a clear assignment between support ticket number and sales order. | X | X | X |  |

|  |
| --- |
| **Declaration of Commitment for the Implementation of Technical and Organizational Measures** |

The Contractor confirms that he implemented the technical and organizational measures for the protection of the Principal's personal data—as described in **Annex 2**—before the commencement of data processing. The Contractor must ensure, regularly monitor and document the fulfillment of these requirements for the duration of the cooperation and must provide this documentation to the Principal on request.

The technical and organizational measures are subject to technical progress and developments. Therefore, the Contractor may implement adequate alternative measures. However, the security level of the specified measures must be maintained. Significant changes must be documented and provided to the Principal on request.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Place, Date |  | Mathias Heese / Managing Director  Martin Behrend / VP Finance  Name of the Contractor / Signature / Company Stamp |